

09/85627

Docket No. 9798423-0006

PATENT

Preliminary Classification:

Proposed Class:

Subclass:

**TRANSMITTAL LETTER TO THE U.S. DESIGNATED OFFICE (DO/US)--  
ENTRY INTO THE U.S. NATIONAL STAGE UNDER CHAPTER I**

PCT/JP00/06308	14 September 2000 (14.09.00)	17 September 1999 (17.09.99)
International Application Number	International Filing Date	International Earliest Priority Date

TITLE OF INVENTION: DATA PROVIDING SYSTEM AND METHOD OF SAME

APPLICANT(S) FOR DO/US: NONAKA, Akira; EZAKI, Tadashi

Box PCT

Assistant Commissioner for Patents

Washington D.C. 20231

ATTENTION: DO/US

---

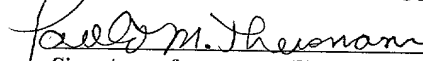
**CERTIFICATION UNDER 37 C.F.R. SECTION 1.10\***

(Express Mail label number is **mandatory**.)(Express Mail certification is **optional**.)

I hereby certify that this paper, along with any document referred to, is being deposited with the United States Postal Service on this date 160501, in an envelope as "Express Mail Post Office to Addressee," mailing Label Number EL67699043405, addressed to the: Assistant Commissioner for Patents, Washington, D.C. 20231.

Paula M. Theismann

(type or print name of person mailing paper)



Signature of person mailing paper

**WARNING:** Certificate of mailing (first class) or facsimile transmission procedures of 37 C.F.R. Section 1.8 cannot be used to obtain a date of mailing or transmission for this correspondence.

**\*WARNING:** Each paper or fee filed by "Express Mail" **must** have the number of the "Express Mail" mailing label placed thereon prior to mailing. 37 C.F.R. Section 1.10(b).  
"Since the filing of correspondence under [Section] 1.10 without the Express Mail mailing label thereon is an oversight that can be avoided by the exercise of reasonable care, requests for waiver of this requirement will **not** be granted on petition." Notice of Oct. 24, 1996, 60 Fed. Reg. 56,439, at 56,442.

0985627-10001-9289580

532 Rec'd PCT/PTO 16 MAY 2001

1. Applicant herewith submits to the United States Designated Office (DO/US) the following items under 35 U.S.C. Section 371:

This express request to immediately begin national examination procedures (35 U.S.C. Section 371(f)).  
The U.S. National Fee (U.S.C. Section 371(c)(1)), as indicated below:

2. Fees

CLAIMS FEE*	(1) FOR	(2) NUMBER FILED	(3) NUMBER EXTRA	(4) RATE	(5) CALCULATIONS
	TOTAL CLAIMS	286 -20 =	266	x \$18.00 =	\$4,788.00
	INDEPENDENT CLAIMS	141 -3 =	138	x \$80.00 =	\$11,040.00
	MULTIPLE DEPENDENT CLAIM(S) (if applicable) + \$270				\$0.00
BASIC FEE	<p>The international search fee, as set forth in Section 1.445(a)(2) to be paid to the US PTO acting as an international Searching Authority</p> <p>where a search report on the international application has been prepared by the European Patent Office or the Japanese Patent Office (37 CFR 1.492(a)(5))</p> <p>..... \$860.00</p>				\$860.00
	Total of above Calculations				= \$16,688.00
SMALL ENTITY	Reduction by 1/2 for filing by small entity, if applicable. Affidavit must be filed (note 37 CFR 1.9, 1.27, 1.28).				- \$0.00
	Subtotal				\$16,688.00
	Total National Fee				\$16,688.00
	Fee for recording the enclosed assignment document \$40.00 (37 CFR 1.21(h)). (See Item below). See attached "ASSIGNMENT COVER SHEET".				\$0.00
TOTAL	Total Fees enclosed				\$16,688.00

A check in the amount of \$16,688.00 to cover the above fees is enclosed.

3. A copy of the International application as filed (35 U.S.C. Section 371(c)(2)) has been transmitted by the International Bureau. Date of mailing of the application from form PCT/IB/308: 29 March 2001.

4. A translation of the International application into the English language (35 U.S.C. Section 371(c)(2)) is transmitted herewith, including 142 sheets of Figures 1-145.

(Transmittal Letter to the United States Designated Office (DO/US - Entry into National Stage under 35 U.S.C. Section 371--

09/856276

532 Rec'd PCT/PTO 16 MAY 2001

5. An oath or declaration, including power of attorney, of the inventor (35 U.S.C. Section 371(c)(4)) complying with 35 U.S.C. Section 115 is submitted herewith unexecuted and such executed oath or declaration will follow.

II. Other document(s) or information included:

6. An international Search Report or Declaration under PCT Article 17(2)(a) is transmitted herewith.

7. An Information Disclosure Statement under 37 C.F.R. Sections 1.97 and 1.98 is transmitted herewith. Also transmitted herewith are Form PTO-1449 (PTO/SB/08A and 08B), and copies of citations listed.

8. Additional documents:

Copy of request (PCT/RO/101)

Copy of PCT/IB/301; 304; 308

Copy of return receipt postcard

**AUTHORIZATION TO CHARGE ADDITIONAL FEES**

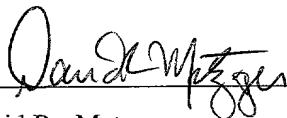
The Commissioner is hereby authorized to charge the following additional fees that may be required by this paper and during the entire pendency of this application to Account No. 19-3140.

37 C.F.R. Section 1.492(a)(1), (2), (3), and (4) (filing fees)

37 C.F.R. Section 1.492(e) and (f) (surcharge fees for filing the declaration and/or filing an English translation of an International Application later than 20 months after the priority date.

Date:

May 16, 2001



David R. Metzger  
Registration No. 32,919  
Sonnenschein Nath & Rosenthal  
P. O. Box 061080  
Wacker Drive Station, Sears Tower  
Chicago, IL 60606-1080  
312-876 8000  
Customer No. 026263

## SPECIFICATION

DATA PROVIDING SYSTEM AND METHOD OF SAME

## 5 TECHNICAL FIELD

The present invention relates to a data providing system providing content data and a method of same, a data providing apparatus, and a data processing apparatus.

## 10 BACKGROUND ART

There is a data providing system for distributing encrypted content data to data processing apparatuses of users concluding predetermined contracts and having the related data processing apparatuses decrypt and reproduce and record the content data.

As one of such data providing systems, there is the conventional EMD (electronic music distribution) system for distributing music data.

Figure 145 is a view of the configuration of a conventional EMD system 700.

In the EMD system 700 shown in Fig. 145, content providers 701a and 701b encrypt content data 704a, 704b, and 704c and copyright information 705a, 705b, and 705c by session key data obtained after mutual certification and supply them to a service provider 710 on-line or



supply by off-line. Here, the copyright information 705a,  
705b, and 705c include for example SCMS (serial copy  
management system) information, electronic watermark  
information requesting burying in the content data, and  
5 information concerning the copyright requesting burying  
in a transmission protocol of the service provider 710.

The service provider 710 decrypts the received  
content data 704a, 704b, and 704c and copyright  
information 705a, 705b, and 705c by using the session key  
10 data.

Then, the service provider 710 buries the copyright  
information 705a, 705b, and 705c in the content data  
704a, 704b, and 704c decrypted or received off-line to  
produce content data 707a, 707b, and 707c. At this time,  
15 the service provider 710 changes predetermined frequency  
domains of for example the electronic watermark  
information among the copyright information 705a, 705b,  
and 705c and buries them in the content data 704a, 704b,  
and 704c and buries the SCMS information in a network  
20 protocol used when transmitting the related content data  
to the user.

Further, the service provider 710 encrypts the  
content data 707a, 707b, and 707c by using content key  
data Kca, Kcb, and Kcc read out from a key database 706.  
25 Thereafter, the service provider 710 encrypts a secure

container 722 storing the encrypted content data 707a,  
707b, and 707c by the session key data obtained after the  
mutual certification and transmits the same to a CA  
(conditional access) module 711 existing in a terminal  
5 709 of the user.

The CA module 711 decrypts the secure container 722  
by using the session key data. Also, the CA module 711  
receives the content key data Kca, Kcb, and Kcc from the  
key database 706 of the service provider 710 by using a  
10 charge function such as an electronic settlement and CA  
and decrypts them by using the session key data. By this,  
in the terminal 709, it becomes possible to decrypt the  
content data 707a, 707b, and 707c by using the content  
key data Kca, Kcb, and Kcc.

15 At this time, the CA module 711 performs charge  
processing in units of content, produces charge  
information 721 in accordance with a result of this, and  
encrypts this by the session key data and then transmits  
the same to a right clearing module 720 of the service  
20 provider 710.

In this case, the CA module 711 collects items to be  
managed by the service provider 710 concerning services  
provided by itself, that is, the contract (update)  
information and the monthly basic fee and other network  
25 rent of the users, performs the charge processing in

units of the content, and ensure security of a physical layer of the network.

The service provider 710 performs distributes profit among the service provider 710 and the content providers 701a, 701b, and 701c when receiving the charge information 721 from the CA module 711.

At this time, the profit is distributed from the service provider 710 to the content providers 701a, 701b, and 701c via for example the JASRAC (Japanese Society for Rights of Authors, Composers, and Publishers). Also, the profit of the content provider is distributed to copyright owner, an artist, a song writer, and/or composer of the related content data and their affiliated production companies by the JASRAC.

Also, in the terminal 709, when recording the content data 707a, 707b, and 707c decrypted by using the content key data Kca, Kcb, and Kcc in a RAM type storage medium 723 or the like, copying is controlled by rewriting SCMS bits of the copyright information 705a, 705b, and 705c. Namely, on the user side, copying is controlled based on the SCMS bits buried in the content data 707a, 707b, and 707c to achieve protection of the copyright.

The SCMS prohibits copying of the content data over for example two generations. Copying of one generation

can be carried out without restriction, however, so there is a problem of insufficient protection of the copyright owner.

Also, in the EMD system 700, the content data not encrypted by the service provider 710 can be technically freely handled, so interested parties of the content provider 710 must monitor actions etc. of the service provider 710, so there are problems in that the load of the related monitoring is large and, at the same time, there is a high possibility of improper loss of the profit of the content provider 701.

Also, in the EMD system 700, it is difficult to restrict acts of the terminal 709 of the user authoring the content data distributed from the service provider 710 and redistributing the same to another terminal etc., so there is the problem of the improper loss of the profit of the content provider 701.

#### DISCLOSURE THE INVENTION

The present invention was made in consideration with the problems of the related art mentioned above and has as an object thereof to provide a data providing system capable of adequately protecting the profit of right holders (interested parties) of the content provider and a method of the same.

Also, another object of the present invention is to

provide a data providing system capable of reducing the load of inspection for protecting the profit of the right holders of the content provider and a method of the same.

To solve the problems of the prior art mentioned  
5 above and achieve the above objects, a data providing system of a first aspect of the present invention is preferably a data providing system for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing  
10 apparatus and the data processing apparatus by a management apparatus, wherein the management apparatus produces a key file storing encrypted content key data and encrypted usage control policy data indicating handling of the content data, the data providing  
15 apparatus provides the content data encrypted by using the content key data, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the key file and determines the handling of the content data based on the related  
20 decrypted usage control policy data.

The mode of operation of the data providing system of the first aspect of the present invention becomes as follows.

In the management apparatus, the key file storing  
25 the encrypted content key data and the encrypted usage

control policy data indicating the handling of the content data is produced, and the related key file is sent to the data providing apparatus.

Then, the content data encrypted by using the  
5 content key data is provided from the data providing apparatus to the data processing apparatus.

Then, in the data processing apparatus, the content key data and the usage control policy data stored in the key file are decrypted, and the handling of the content  
10 data is determined based on the related decrypted usage control policy data.

Also, a data providing system of a second aspect of the present invention is a data providing system for distributing content data from a data providing apparatus  
15 to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, wherein the management apparatus produces a key file storing encrypted content key data and encrypted usage control policy data indicating  
20 handling of the content data, the data providing apparatus distributes a module storing a content file storing the content data encrypted by using the content key data and the key file received from the management apparatus to the data processing apparatus, and the data  
25 processing apparatus decrypts the content key data and

the usage control policy data stored in the distributed module and determines the handling of the content data based on the related decrypted usage control policy data.

The mode of operation of the data providing system  
5 of the second aspect of the present invention becomes as follows.

In the management apparatus, the key file storing the encrypted content key data and the encrypted usage control policy data indicating the handling of the  
10 content data is produced.

Then, the related produced key file is distributed from the management apparatus to the data providing apparatus.

Then, the module storing the content file storing  
15 the content data encrypted by using the content key data and the key file received from the management apparatus is distributed from the data providing apparatus to the data processing apparatus.

Then, in the data processing apparatus, the content  
20 key data and the usage control policy data stored in the distributed module are decrypted, and the handling of the content data is determined based on the related decrypted usage control policy data.

A data providing system of a third aspect of the  
25 present invention is a data providing system for

distributing content data from a data providing apparatus  
to a data processing apparatus and managing the data  
providing apparatus and the data processing apparatus by  
a management apparatus, wherein the management apparatus  
5 produces a key file storing encrypted content key data  
and encrypted usage control policy data indicating  
handling of the content data, the data providing  
apparatus distributes a module storing a content file  
containing content data encrypted by using the content  
10 key data and the key file received from the management  
apparatus to the data processing apparatus, and the data  
processing apparatus decrypts the content key data and  
the usage control policy data stored in the distributed  
module and determines the handling of the content data  
15 based on the related decrypted usage control policy data.

The mode of operation of the data providing system  
of the third aspect of the present invention becomes as  
follows.

In the management apparatus, the key file storing  
20 the encrypted content key data and the encrypted usage  
control policy data indicating the handling of the  
content data is produced, and the related produced key  
file is sent to the data providing apparatus.

Then, the module storing the content file containing  
25 the content data encrypted by using the content key data



and the key file received from the management apparatus is distributed from the data providing apparatus to the data processing apparatus.

Then, in the data processing apparatus, the content  
5 key data and the usage control policy data stored in the distributed module are decrypted, and the handling of the content data is determined based on the related decrypted usage control policy data.

Also, a data providing system of a fourth aspect of  
10 the present invention is a data providing system for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, wherein the management apparatus  
15 produces a key file storing encrypted content key data and encrypted usage control policy data indicating handling of the content data, the data providing apparatus individually distributes the content file storing the content data encrypted by using the content  
20 key data and the key file received from the management apparatus to the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key file and determines the handling of the content data  
25 stored in the distributed content file based on the

related decrypted usage control policy data.

The mode of operation of the data providing system of the fourth aspect of the present invention becomes as follows.

5        In the management apparatus, the key file storing the encrypted content key data and the encrypted usage control policy data indicating the handling of the content data is produced, and the related produced key file is sent to the data providing apparatus.

10       Then, in the data providing apparatus, the content file storing the content data encrypted by using the content key data and the key file received from the management apparatus are distributed.

15       Then, in the data processing apparatus, the content key data and the usage control policy data stored in the distributed key file are decrypted, and the handling of the content data stored in the distributed content file is determined based on the related decrypted usage control policy data.

20       Also, a data providing system of a fifth aspect of the present invention is a data providing system for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by  
25       a management apparatus, wherein the management apparatus

produces a key file storing encrypted content key data  
and encrypted usage control policy data indicating  
handling of the content data and distributes the related  
produced key file to the data processing apparatus, the  
5 data providing apparatus distributes a content file  
storing the content data encrypted by using the content  
key data to the data processing apparatus, and the data  
processing apparatus decrypts the content key data and  
the usage control policy data stored in the distributed  
10 key file and determines the handling of the content data  
stored in the distributed content file based on the  
related decrypted usage control policy data.

The mode of operation of the data providing system  
of the fifth aspect of the present invention becomes as  
15 follows.

In the management apparatus, the key file storing  
the encrypted content key data and the encrypted usage  
control policy data indicating the handling of the  
content data is produced.

20 The related produced key file is distributed from  
the management apparatus to the data processing  
apparatus.

Also, the content file storing the content data  
encrypted by using the content key data is distributed  
25 from the data providing apparatus to the data processing

apparatus.

Then, in the data processing apparatus, the content key data and the usage control policy data stored in the distributed key file are decrypted, and the handling of the content data stored in the distributed content file is determined based on the related decrypted usage control policy data.

Also, a data providing system of a sixth aspect of the present invention is a data providing system for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, wherein the management apparatus produces a key file storing encrypted content key data and encrypted usage control policy data indicating handling of the content data, the data providing apparatus distributes a module storing the content data encrypted by using the content key data and the key file received from the management apparatus to the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed module and determines the handling of the content data based on the related decrypted usage control policy data.

The mode of operation of the data providing system

of the sixth aspect of the present invention becomes as follows.

In the management apparatus, the key file storing the encrypted content key data and the encrypted usage control policy data indicating the handling of the content data is produced, and the related produced key file is sent to the data providing apparatus.

Then, the module storing the content data encrypted by using the content key data and the key file received from the management apparatus is distributed from the data providing apparatus to the data processing apparatus.

Then, in the data processing apparatus, the content key data and the usage control policy data stored in the distributed module are decrypted, and the handling of the content data is determined based on the related decrypted usage control policy data.

Also, a data providing system of a seventh aspect of the present invention is a data providing system for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, wherein the management apparatus produces a key file storing encrypted content key data and encrypted usage control policy data indicating

handling of the content data, the data providing  
apparatus individually distributes the content data  
encrypted by using the content key data and the key file  
received from the management apparatus to the data  
5 processing apparatus, and the data processing apparatus  
decrypts the content key data and the usage control  
policy data stored in the distributed key file and  
determines the handling of the distributed content data  
based on the related decrypted usage control policy data.

10 The mode of operation of the data providing system  
of the seventh aspect of the present invention becomes as  
follows.

In the management apparatus, the key file storing  
the encrypted content key data and the encrypted usage  
15 control policy data indicating the handling of the  
content data is produced, and the related produced key  
file is sent to the data providing apparatus.

Then, the content data encrypted by using the  
content key data and the key file received from the  
20 management apparatus are individually distributed from  
the data providing apparatus to the data processing  
apparatus.

Then, in the data processing apparatus, the content  
key data and the usage control policy data stored in the  
25 distributed key file are decrypted, and the handling of

the distributed content data is determined based on the related decrypted usage control policy data.

Also, a data providing system of an eighth aspect of the present invention is a data providing system for  
5 distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, wherein the management apparatus produces a key file storing encrypted content key data  
10 and encrypted usage control policy data indicating handling of the content data and distributes the related produced key file to the data processing apparatus, the data processing apparatus distributes the content data encrypted by using the content key data to the data  
15 processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key file and determines the handling of the distributed content data based on the related decrypted usage control policy data.

20 The mode of operation of the data providing system of the eighth aspect of the present invention becomes as follows.

In the management apparatus, the key file storing the encrypted content key data and the encrypted usage  
25 control policy data indicating the handling of the

0955276-10004  
FOUO 9228350

content data is produced, and the related produced key file is sent to the data processing apparatus.

Also, the content data encrypted by using the content key data are distributed from the data providing apparatus to the data processing apparatus.

Then, in the data processing apparatus, the content key data and the usage control policy data stored in the distributed key file are decrypted, and the handling of the distributed content data is determined based on the related decrypted usage control policy data.

Also, a data providing system of a ninth aspect of the present invention is a data providing system for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, wherein the management apparatus produces encrypted content key data and encrypted usage control policy data indicating handling of the content data, the data providing apparatus individually distributes the content data encrypted by using the content key data, the encrypted content key data received from the management apparatus, and the encrypted usage control policy data to the data processing apparatus, and the data processing apparatus decrypts the distributed content key data and the usage control policy data and



determines the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

The mode of operation of the data providing system  
5 of the ninth aspect of the present invention becomes as follows.

In the management apparatus, the encrypted content key data and the encrypted usage control policy data indicating the handling of the content data are produced,  
10 and they are sent to the data providing apparatus.

Then, the content data encrypted by using the content key data and the encrypted content key data and the encrypted usage control policy data received from the management apparatus are individually distributed from  
15 the data providing apparatus to the data processing apparatus.

Then, in the data processing apparatus, the distributed content key data and the usage control policy data are decrypted, and the handling of the content data  
20 stored in the distributed content file is determined based on the related decrypted usage control policy data.

Also, a data providing system of a 10th aspect of the present invention is a data providing system for distributing content data from a data providing apparatus  
25 to a data processing apparatus and managing the data

providing apparatus and the data processing apparatus by  
a management apparatus, wherein the management apparatus  
produces encrypted content key data and encrypted usage  
control policy data indicating handling of the content  
5 data and distributes the same to the data processing  
apparatus, the data providing apparatus distributes the  
content data encrypted by using the content key data to  
the data processing apparatus, and the data processing  
apparatus decrypts the distributed content key data and  
10 the usage control policy data and determines the handling  
of the distributed content data based on the related  
decrypted usage control policy data.

The mode of operation of the data providing system  
of the 10th aspect of the present invention becomes as  
15 follows.

In the management apparatus, the encrypted content  
key data and the encrypted usage control policy data  
indicating the handling of the content data are produced,  
and they are sent to the data processing apparatus.

20 Also, the content data encrypted by using the  
content key data are distributed from the data providing  
apparatus to the data processing apparatus.

Then, in the data processing apparatus, the  
distributed content key data and the usage control policy  
25 data are decrypted, and the handling of the distributed

content data is determined based on the related decrypted usage control policy data.

Also, a data providing system of an 11th aspect of the present invention is a data providing system having a data providing apparatus, a data distribution apparatus, a data processing apparatus, and a management apparatus, wherein the management apparatus produces a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, the data providing apparatus provides the content data encrypted by using the content key data, the data distribution apparatus distributes the provided content data to the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the key file and determines the handling of the distributed content data based on the related decrypted usage control policy data.

The mode of operation of the data providing system of the 11th aspect of the present invention becomes as follows.

In the management apparatus, the key file storing the encrypted content key data and the encrypted usage control policy data indicating the handling of the content data is produced.

Then, the content data encrypted by using the content key data is provided from the data providing apparatus to the data distribution apparatus.

Then, the provided content data is distributed from  
5 the data distribution apparatus to the data processing apparatus.

Then, in the data processing apparatus, the content key data and the usage control policy data stored in the key file are decrypted, and the handling of the  
10 distributed content data is determined based on the related decrypted usage control policy data.

Also, a data providing system of a 12th aspect of the present invention is a data providing system for providing content data from a data providing apparatus to  
15 a data distribution apparatus, distributing the content data from the data distribution apparatus to a data processing apparatus, and managing the data providing apparatus, the data distribution apparatus, and the data processing apparatus by a management apparatus, wherein  
20 the management apparatus produces a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, the data providing apparatus provides a first module storing a content file storing the content data encrypted  
25 by using the content key data and the key file received

from the management apparatus to the data distribution apparatus, the data distribution apparatus distributes a second module storing the provided content file and the key file to the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed second module and determines the handling of the content data stored in the distributed second module based on the related decrypted usage control policy data.

10       The mode of operation of the data providing system of the 12th aspect of the present invention becomes as follows.

15       In the management apparatus, the key file storing the encrypted content key data and the encrypted usage control policy data indicating the handling of the content data is produced, and the related produced key file is sent to the data providing apparatus.

20       Then, the first module storing the content file storing the content data encrypted by using the content key data and the key file received from the management apparatus is provided from the data providing apparatus to the data distribution apparatus.

25       Then, the second module storing the provided content file and the key file is distributed from the data distribution apparatus to the data processing apparatus.

Then, in the data processing apparatus, the content key data and the usage control policy data stored in the distributed second module are decrypted, and the handling of the content data stored in the distributed second  
5 module is determined based on the related decrypted usage control policy data.

Also, a data providing system of a 13th aspect of the present invention is a data providing system for providing content data from a data providing apparatus to  
10 a data distribution apparatus, distributing the content data from the data distribution apparatus to a data processing apparatus, and managing the data providing apparatus, the data distribution apparatus, and the data processing apparatus by a management apparatus, wherein  
15 the management apparatus produces a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, the data providing apparatus provides a first module storing a content file containing the content data  
20 encrypted by using the content key data and a key file received from the management apparatus to the data distribution apparatus, the data distribution apparatus distributes a second module storing the provided content file to the data processing apparatus, and the data  
25 processing apparatus decrypts the content key data and

the usage control policy data stored in the distributed second module and determines the handling of the content data stored in the distributed second module based on the related decrypted usage control policy data.

5       Also, a data providing system of a 14th aspect of the present invention is a data providing system for providing content data from a data providing apparatus to a data distribution apparatus, distributing the content data from the data distribution apparatus to a data processing apparatus, and managing the data providing apparatus, the data distribution apparatus, and the data processing apparatus by a management apparatus, wherein the management apparatus produces a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, the data providing apparatus individually distributes a content file storing the content data encrypted by using the content key data and the key file received from the management apparatus to the data distribution apparatus, the data distribution apparatus individually distributes the distributed content file and key file to the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key file and determines the handling of the content data stored in the

10

15

20

25

distributed content file based on the related decrypted usage control policy data.

Also, a data providing system of a 15th aspect of the present invention is a data providing system for  
5 distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, wherein the management apparatus produces a key file storing encrypted content key data  
10 and encrypted usage control policy data indicating the handling of the content data and distributes the related produced key file to the data processing apparatus, the data providing apparatus provides a content file storing the content data encrypted by using the content key data  
15 to the data distribution apparatus, the data distribution apparatus distributes the provided content file to the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key file  
20 and determines the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

Also, a data providing system of a 16th aspect of the present invention is a data providing system for  
25 providing content data from a data providing apparatus to



a data distribution apparatus, distributing the content data from the data distribution apparatus to a data processing apparatus, and managing the data providing apparatus, the data distribution apparatus, and the data processing apparatus by a management apparatus, wherein the management apparatus produces a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, the data providing apparatus provides a first module storing the content data encrypted by using the content key data and the key file received from the management apparatus to the data distribution apparatus, the data distribution apparatus distributes a second module storing the provided content data and the key file to the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed second module and determines the handling of the content data stored in the distributed second module based on the related decrypted usage control policy data.

Also, a data providing system of a 17th aspect of the present invention is a data providing system for providing content data from a data providing apparatus to a data distribution apparatus, distributing the content data from the data distribution apparatus to a data

processing apparatus, and managing the data providing  
apparatus, the data distribution apparatus, and the data  
processing apparatus by a management apparatus, wherein  
the management apparatus produces a key file storing  
5 encrypted content key data and encrypted usage control  
policy data indicating the handling of the content data,  
the data providing apparatus individually distributes the  
content data encrypted by using the content key data and  
the key file received from the management apparatus to  
10 the data distribution apparatus, the data distribution  
apparatus individually distributes the distributed  
content data and the key file to the data distribution  
apparatus, and the data processing apparatus decrypts the  
content key data and the usage control policy data stored  
15 in the distributed key file and determines the handling  
of the distributed content data based on the related  
decrypted usage control policy data.

Also, a data providing system of an 18th aspect of  
the present invention is a data providing system for  
20 distributing content data from a data providing apparatus  
to a data processing apparatus and managing the data  
providing apparatus and the data processing apparatus by  
a management apparatus, wherein the management apparatus  
produces a key file storing encrypted content key data  
25 and encrypted usage control policy data indicating the

handling of the content data and distributes the related  
produced key file to the data processing apparatus, the  
data processing apparatus provides the content data  
encrypted by using the content key data to the data  
5 distribution apparatus, the data distribution apparatus  
distributes the provided content data to the data  
processing apparatus, and the data processing apparatus  
decrypts the content key data and the usage control  
policy data stored in the distributed key file and  
10 determines the handling of the distributed content data  
based on the related decrypted usage control policy data.

Also, a data providing system of a 19th aspect of  
the present invention is a data providing system for  
providing content data from a data providing apparatus to  
15 a data distribution apparatus, distributing the content  
data from the data distribution apparatus to a data  
processing apparatus, and managing the data providing  
apparatus, the data distribution apparatus, and the data  
processing apparatus by a management apparatus, wherein  
20 the management apparatus provides encrypted content key  
data and encrypted usage control policy data indicating  
the handling of the content data to the data providing  
apparatus, the data providing apparatus individually  
distributes the content data encrypted by using the  
25 content key data and the encrypted content key data and

the encrypted usage control policy data received from the management apparatus to the data distribution apparatus, the data distribution apparatus individually distributes the distributed content data, the encrypted content key data, and the encrypted usage control policy data to the data distribution apparatus, and the data processing apparatus decrypts the distributed content key data and the usage control policy data and determines the handling of the distributed content data based on the related decrypted usage control policy data.

Also, a data providing system of a 20th aspect of the present invention is a data providing system for providing content data from a data providing apparatus to a data distribution apparatus, distributing the content data from the data distribution apparatus to a data processing apparatus, and managing the data providing apparatus, the data distribution apparatus, and the data processing apparatus by a management apparatus, wherein the management apparatus provides encrypted content key data and encrypted usage control policy data indicating the handling of the content data to the data processing apparatus, the data providing apparatus provides the content data encrypted by using the content key data to the data distribution apparatus, the data distribution apparatus distributes the provided content data to the

data processing apparatus, and the data processing  
apparatus decrypts the distribute the content key data  
and the usage control policy data and determines the  
handling of the distributed content data based on the  
5 related decrypted usage control policy data.

Also, a data providing system of a 21st aspect of  
the present invention is a data providing system having a  
data providing apparatus, a data distribution apparatus,  
a management apparatus, and a data processing apparatus,  
10 wherein the data providing apparatus provides master  
source data of content to the management apparatus, the  
management apparatus manages the data providing  
apparatus, the data distribution apparatus, and the data  
processing apparatus, encrypts the provided master source  
15 data by using content key data to produce content data,  
produces a content file storing the related content data,  
produces a key file storing the encrypted content key  
data and encrypted usage control policy data indicating  
the handling of the content data, and provides the  
20 content file and the key file to the data distribution  
apparatus, the data distribution apparatus distributes  
the provided content file and the key file to the data  
processing apparatus, and the data processing apparatus  
decrypts the content key data and the usage control  
25 policy data stored in the distributed key file and

determines the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

Also, a data providing system of a 22nd aspect of  
5 the present invention is a data providing system having a data providing apparatus, a data distribution apparatus, a management apparatus, and a data processing apparatus, wherein the data providing apparatus provides master source data of content to the management apparatus, the  
10 management apparatus manages the data providing apparatus, the data distribution apparatus, and the data processing apparatus, encrypts the provided master source data by using content key data to produce content data, produces a content file storing the related content data,  
15 produces a key file storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data, and provides the content file to the data distribution apparatus, provides the key file to the data processing apparatus, the data  
20 distribution apparatus distributes the provided content file to the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key file and determines the handling of the content data  
25 stored in the distributed content file based on the

related decrypted usage control policy data.

Also, a data providing system of a 23rd aspect of the present invention is a data providing system having a data providing apparatus, a data distribution apparatus, 5 a management apparatus, and a data processing apparatus, wherein the data providing apparatus provides a content file storing encrypted content data using content key data to the management apparatus, the management apparatus manages the data providing apparatus, the data 10 distribution apparatus, and the data processing apparatus, produces a key file storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data, and provides the content file provided from the data providing 15 apparatus and the produced key file to the data distribution apparatus, the data distribution apparatus distributes the provided content file and the key file to the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage 20 control policy data stored in the distributed key file and determines the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

Also, a data providing system of a 24th aspect of 25 the present invention is a data providing system having a

data providing apparatus, a data distribution apparatus,  
a management apparatus, and a data processing apparatus,  
wherein the data providing apparatus provides a content  
file storing encrypted content data using content key  
5 data to the management apparatus, the management  
apparatus manages the data providing apparatus, the data  
distribution apparatus, and the data processing  
apparatus, produces a key file storing the encrypted  
content key data and encrypted usage control policy data  
10 indicating the handling of the content data, provides the  
content file provided from the data providing apparatus  
to the data distribution apparatus, and provides the  
produced key file to the data processing apparatus, the  
data distribution apparatus distributes the provided  
15 content file to the data processing apparatus, and the  
data processing apparatus decrypts the content key data  
and the usage control policy data stored in the provided  
key file and determines the handling of the content data  
stored in the distributed content file based on the  
20 related decrypted usage control policy data.

Also, a data providing system of a 25th aspect of  
the present invention is a data providing system having a  
data providing apparatus, a data distribution apparatus,  
a management apparatus, a database device, and a data  
25 processing apparatus, wherein the data providing



apparatus encrypts content data by using content key data, produces a content file storing the related encrypted content data, and stores the related produced content file and a key file provided from the management apparatus in the database device, the management apparatus produces the key file storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data, and provides the related produced key file to the data providing apparatus, the data distribution apparatus distributes the content file and key file obtained from the database device to the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key file and determines the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

Also, a data providing system of a 26th aspect of the present invention is a data providing system having a data providing apparatus, a data distribution apparatus, a management apparatus, a database device, and a data processing apparatus, wherein the data providing apparatus encrypts content data by using content key data, produces a content file storing the related encrypted content data, and stores the related produced

content file in the database device, the management apparatus produces the key file storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data and provides  
5 the related produced key file to the data distribution apparatus, the data distribution apparatus distributes the content file obtained from the database device and the key file provided from the data distribution apparatus to the data processing apparatus, and the data  
10 processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key file and determines the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

15 Also, a data providing system of a 27th aspect of the present invention is a data providing system having a data providing apparatus, a data distribution apparatus, a management apparatus, a database device, and a data processing apparatus, wherein the data providing  
20 apparatus encrypts content data by using content key data, produces a content file storing the related encrypted content data, and stores the related produced content file in the database device, the management apparatus produces the key file storing the encrypted  
25 content key data and encrypted usage control policy data

indicating the handling of the content data and provides  
the related produced key file to the data processing  
apparatus, the data distribution apparatus distributes  
the content file obtained from the database device and  
5 the key file provided from the data distribution  
apparatus to the data processing apparatus, and the data  
processing apparatus decrypts the content key data and  
the usage control policy data stored in the provided key  
file and determines the handling of the content data  
10 stored in the distributed content file based on the  
related decrypted usage control policy data.

Also, a data providing system of a 28th aspect of  
the present invention is a data providing system having a  
plurality of data providing apparatuses, a data  
15 distribution apparatus, a plurality of management  
apparatuses, a database device, and a data processing  
apparatus, wherein the data providing apparatuses encrypt  
content data by using content key data, produce content  
files storing the related encrypted content data, and  
20 store the related produced content files and key files  
provided from corresponding management apparatuses in the  
database device, the management apparatuses produce key  
files storing the encrypted content key data and the  
encrypted usage control policy data indicating the  
25 handling of the content data for the content data

provided by corresponding data providing apparatuses, and provide the related produced key files to corresponding data providing apparatuses, the data distribution apparatus distributes the content files and key files

5 obtained from the database device to the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key files and determines the handling of the content data stored in the distributed content  
10 files based on the related decrypted usage control policy data.

Also, a data providing system of a 29th aspect of the present invention is a data providing system having a plurality of data providing apparatuses, a data  
15 distribution apparatus, a plurality of management apparatuses, a database device, and a data processing apparatus, wherein the data providing apparatuses encrypt content data by using content key data, produce content files storing the related encrypted content data, and  
20 store the related produced content files in the database device, the management apparatuses produce key files storing the encrypted content key data and the encrypted usage control policy data indicating the handling of the content data for the content data provided by  
25 corresponding data providing apparatuses, and provide the

related produced key files to the data distribution apparatus, the data distribution apparatus distributes the content files obtained from the database device and the key files provided from the management apparatus to  
5 the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key files and determines the handling of the content data stored in the distributed content files based on the related  
10 decrypted usage control policy data.

Also, a data providing system of a 30th aspect of the present invention is a data providing system having a plurality of data providing apparatuses, a data distribution apparatus, a plurality of management  
15 apparatuses, a database device, and a data processing apparatus, wherein the data providing apparatuses encrypt content data by using content key data, produce content files storing the related encrypted content data, and store the related produced content files in the database  
20 device, the management apparatuses produce key files storing the encrypted content key data and the encrypted usage control policy data indicating the handling of the content data for the content data provided by corresponding data providing apparatuses, and provide the  
25 related produced key files to the data processing

apparatus, the data distribution apparatus distributes the content files obtained from the database device to the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key files and determines the handling of the content data stored in the distributed content files based on the related decrypted usage control policy data.

Also, a data providing system of a 31st aspect of the present invention is a data providing system having a plurality of data providing apparatuses, a data distribution apparatus, a plurality of management apparatuses, a database device, and a data processing apparatus, wherein the data providing apparatuses provide master sources of content data to corresponding management apparatuses and store content files and key files received from the related management apparatuses in the database, the management apparatuses encrypt the master sources received from corresponding data providing apparatuses by using content key data, produce the content files storing the related encrypted content data, produce key files storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data for the content data provided by corresponding data providing apparatuses, and

send the produced content files and the produced key files to corresponding data providing apparatuses, the data distribution apparatus distributes the content files and key files obtained from the database device to the

5 data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key files and determines the handling of the content data stored in the distributed content files based on the related

10 decrypted usage control policy data.

Also, a data providing system of a 32nd aspect of the present invention is a data providing system having a plurality of data providing apparatuses, a data distribution apparatus, a plurality of management

15 apparatuses, a database device, and a data processing apparatus, wherein the data providing apparatuses provide master sources of content data to corresponding management apparatuses, and store content files received from the related management apparatuses in the database,

20 the management apparatuses encrypt the master sources received from corresponding data providing apparatuses by using content key data, produce the content files storing the related encrypted content data, send the related produced content files to the data providing apparatuses,

25 produce key files storing the encrypted content key data

and encrypted usage control policy data indicating the handling of the content data for the content data provided by corresponding data providing apparatuses, and send the produced key files to corresponding data

5 distribution apparatus, the data distribution apparatus distributes the content files obtained from the database device and the key files provided from the management apparatuses to the data processing apparatus, and the data processing apparatus decrypts the content key data  
10 and the usage control policy data stored in the distributed key files and determines the handling of the content data stored in the distributed content files based on the related decrypted usage control policy data.

Also, a data providing system of a 33rd aspect of  
15 the present invention is a data providing system having a plurality of data providing apparatuses, a data distribution apparatus, a plurality of management apparatuses, a database device, and a data processing apparatus, wherein the data providing apparatuses provide  
20 master sources of content data to corresponding management apparatuses and store content files received from the related management apparatuses in the database, the management apparatuses encrypt the master sources received from corresponding data providing apparatuses by  
25 using content key data, produce the content files storing



the related encrypted content data, send the related  
produced content files to the data providing apparatuses,  
produce key files storing the encrypted content key data  
and encrypted usage control policy data indicating the  
5 handling of the content data for the content data  
provided by corresponding data providing apparatuses, and  
send the produced key files to the data processing  
apparatus, the data distribution apparatus distributes  
the content files obtained from the database device and  
10 the key files provided from the management apparatuses to  
the data processing apparatus, and the data processing  
apparatus decrypts the content key data and the usage  
control policy data stored in the provided key files and  
determines the handling of the content data stored in the  
15 distributed content files based on the related decrypted  
usage control policy data.

Also, a data providing method of a first aspect of  
the present invention is a data providing method for  
distributing content data from a data providing apparatus  
20 to a data processing apparatus and managing the data  
providing apparatus and the data processing apparatus by  
a management apparatus, wherein the management apparatus  
produces a key file storing encrypted content key data  
and encrypted usage control policy data indicating the  
25 handling of the content data, the data providing

apparatus provides the content data encrypted by using  
the content key data, and the data processing apparatus  
decrypts the content key data and the usage control  
policy data stored in the key file and determines the  
5 handling of the content data based on the related  
decrypted usage control policy data.

Also, a data providing method of a second aspect of  
the present invention is a data providing method for  
distributing content data from a data providing apparatus  
10 to a data processing apparatus and managing the data  
providing apparatus and the data processing apparatus by  
a management apparatus, comprising the steps of, in the  
management apparatus, preparing a key file storing  
encrypted content key data and encrypted usage control  
15 policy data indicating the handling of the content data,  
distributing the produced key file from the management  
apparatus to the data providing apparatus, distributing a  
module storing a content file storing the content data  
encrypted by using the content key data and the key file  
20 distributed from the management apparatus from the data  
providing apparatus to the data processing apparatus, and  
in the data processing apparatus, decrypting the content  
key data and the usage control policy data stored in the  
distributed module and determining the handling of the  
25 content data based on the related decrypted usage control

policy data.

Also, a data providing method of a third aspect of the present invention is a data providing method for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, comprising the steps of, in the management apparatus, preparing a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, in the data providing apparatus, distributing a module storing a content file containing the content data encrypted by using the content key data and the key file received from the management apparatus to the data processing apparatus, and in the data processing apparatus, decrypting the content key data and the usage control policy data stored in the distributed module and determining the handling of the content data based on the related decrypted usage control policy data.

Also, a data providing method of a fourth aspect of the present invention is a data providing method for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, comprising the steps of, in the

management apparatus, preparing a key file storing  
encrypted content key data and encrypted usage control  
policy data indicating the handling of the content data,  
distributing the related key file from the management  
5 apparatus to the data providing apparatus, individually  
distributing a content file storing the content data  
encrypted by using the content key data and the key file  
received from the management apparatus from the data  
providing apparatus to the data processing apparatus, and  
10 in the data processing apparatus, decrypting the content  
key data and the usage control policy data stored in the  
distributed key file and determining the handling of the  
content data stored in the distributed content file based  
on the related decrypted usage control policy data.

15 Also, a data providing method of a fifth aspect of  
the present invention is a data providing method for  
distributing content data from a data providing apparatus  
to a data processing apparatus and managing the data  
providing apparatus and the data processing apparatus by  
20 a management apparatus, comprising the steps of, in the  
management apparatus, preparing a key file storing  
encrypted content key data and encrypted usage control  
policy data indicating the handling of the content data,  
distributing the related key file from the management  
25 apparatus to the data processing apparatus, distributing

a content file storing the content data encrypted by  
using the content key data from the data providing  
apparatus to the data processing apparatus, and in the  
data processing apparatus, decrypting the content key  
5 data and the usage control policy data stored in the  
distributed key file and determining the handling of the  
content data stored in the distributed content file based  
on the related decrypted usage control policy data.

Also, a data providing method of a sixth aspect of  
10 the present invention is a data providing method for  
distributing content data from a data providing apparatus  
to a data processing apparatus and managing the data  
providing apparatus and the data processing apparatus by  
a management apparatus, comprising the steps of, in the  
15 management apparatus, preparing a key file storing  
encrypted content key data and encrypted usage control  
policy data indicating the handling of the content data,  
in the data providing apparatus, distributing a module  
storing the content data encrypted by using the content  
20 key data and the key file received from the management  
apparatus to the data processing apparatus, and in the  
data processing apparatus, decrypting the content key  
data and the usage control policy data stored in the  
distributed module and determining the handling of the  
25 content data based on the related decrypted usage control

policy data.

Also, a data providing method of a seventh aspect of the present invention is a data providing method for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, comprising the steps of, in the management apparatus, preparing a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, in the data providing apparatus, individually distributing the content data encrypted by using the content key data and the key file received from the management apparatus to the data processing apparatus, and in the data processing apparatus, decrypting the content key data and the usage control policy data stored in the distributed key file and determining the handling of the distributed content data based on the related decrypted usage control policy data.

Also, a data providing method of an eighth aspect of the present invention is a data providing method for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, comprising the steps of, in the

management apparatus, preparing a key file storing  
encrypted content key data and encrypted usage control  
policy data indicating the handling of the content data,  
distributing the related produced key file to the data  
5 processing apparatus, in the data providing apparatus,  
distributing the content data encrypted by using the  
content key data to the data processing apparatus, and in  
the data processing apparatus, decrypting the content key  
data and the usage control policy data stored in the  
10 distributed key file and determining the handling of the  
distributed content data based on the related decrypted  
usage control policy data.

Also, a data providing method of a ninth aspect of  
the present invention is a data providing method for  
15 distributing content data from a data providing apparatus  
to a data processing apparatus and managing the data  
providing apparatus and the data processing apparatus by  
a management apparatus, comprising the steps of, in the  
management apparatus, preparing encrypted content key  
20 data and encrypted usage control policy data indicating  
the handling of the content data, in the data providing  
apparatus, individually distributing the content data  
encrypted by using the content key data and the encrypted  
content key data and the encrypted usage control policy  
25 data received from the management apparatus to the data

processing apparatus, and in the data processing  
apparatus, decrypting the distributed content key data  
and the usage control policy data and determining the  
handling of the content data stored in the distributed  
5 content file based on the related decrypted usage control  
policy data.

Also, a data providing method of a 10th aspect of  
the present invention is a data providing method for  
distributing content data from a data providing apparatus  
10 to a data processing apparatus and managing the data  
providing apparatus and the data processing apparatus by  
a management apparatus, comprising the steps of, in the  
management apparatus, preparing encrypted content key  
data and encrypted usage control policy data indicating  
15 the handling of the content data and distributing the  
same to the data processing apparatus, in the data  
providing apparatus, distributing the content data  
encrypted by using the content key data to the data  
processing apparatus, and in the data processing  
20 apparatus, decrypting the distributed content key data  
and the usage control policy data and determining the  
handling of the distributed content data based on the  
related decrypted usage control policy data.

Also, a data providing method of an 11th aspect of  
25 the present invention is a data providing method using a



data providing apparatus, a data distribution apparatus,  
a data processing apparatus, and a management apparatus,  
comprising the steps of, in the management apparatus,  
preparing a key file storing encrypted content key data  
5 and encrypted usage control policy data indicating the  
handling of the content data, providing the content data  
encrypted by using the content key data from the data  
providing apparatus to the data distribution apparatus,  
in the data distribution apparatus, distributing the  
10 provided content data to the data processing apparatus,  
and in the data processing apparatus, decrypting the  
content key data and the usage control policy data stored  
in the key file and determining the handling of the  
distributed content data based on the related decrypted  
15 usage control policy data.

Also, a data providing method of a 12th aspect of  
the present invention is a data providing method for  
providing content data from a data providing apparatus to  
a data distribution apparatus, distributing the content  
20 data from the data distribution apparatus to a data  
processing apparatus, and managing the data providing  
apparatus, the data distribution apparatus, and the data  
processing apparatus by a management apparatus,  
comprising the steps of, in the management apparatus,  
25 preparing a key file storing encrypted content key data

and encrypted usage control policy data indicating the handling of the content data, distributing the related produced key file from the management apparatus to the data providing apparatus, providing a first module

5 storing a content file storing the content data encrypted by using the content key data and the key file received from the management apparatus from the data providing apparatus to the data distribution apparatus, and distributing a second module storing the provided content

10 file and the key file from the data distribution apparatus to the data processing apparatus, and in the data processing apparatus, decrypting the content key data and the usage control policy data stored in the distributed second module and determining the handling of

15 the content data stored in the distributed second module based on the related decrypted usage control policy data.

Also, a data providing method of a 13th aspect of the present invention is a data providing method for providing content data from a data providing apparatus to

20 a data distribution apparatus, distributing the content data from the data distribution apparatus to a data processing apparatus, and managing the data providing apparatus, the data distribution apparatus, and the data processing apparatus by a management apparatus,

25 comprising the steps of, in the management apparatus,

preparing a key file storing encrypted content key data  
and encrypted usage control policy data indicating the  
handling of the content data, in the data providing  
apparatus, providing a first module storing a content  
5 file containing the content data encrypted by using the  
content key data and a key file received from the  
management apparatus to the data distribution apparatus,  
in the data distribution apparatus, distributing a second  
module storing the provided content file to the data  
10 processing apparatus, and in the data processing  
apparatus, decrypting the content key data and the usage  
control policy data stored in the distributed second  
module and determining the handling of the content data  
stored in the distributed second module based on the  
15 related decrypted usage control policy data.

Also, a data providing method of a 14th aspect of  
the present invention is a data providing method for  
providing content data from a data providing apparatus to  
a data distribution apparatus, distributing the content  
20 data from the data distribution apparatus to a data  
processing apparatus, and managing the data providing  
apparatus, the data distribution apparatus, and the data  
processing apparatus by a management apparatus,  
comprising the steps of, in the management apparatus,  
25 preparing a key file storing encrypted content key data

and encrypted usage control policy data indicating the  
handling of the content data, distributing the produced  
key file from the management apparatus to the data  
providing apparatus, individually distributing a content  
5 file storing the content data encrypted by using the  
content key data and the key file received from the  
management apparatus from the data providing apparatus to  
the data distribution apparatus, individually  
distributing the distributed content file and the key  
10 file from the data distribution apparatus to the data  
distribution apparatus, and in the data processing  
apparatus, decrypting the content key data and the usage  
control policy data stored in the distributed key file  
and determining the handling of the content data stored  
15 in the distributed content file based on the related  
decrypted usage control policy data.

Also, a data providing method of a 15th aspect of  
the present invention is a data providing method for  
distributing content data from a data providing apparatus  
20 to a data processing apparatus and managing the data  
providing apparatus and the data processing apparatus by  
a management apparatus, comprising the steps of, in the  
management apparatus, preparing a key file storing  
encrypted content key data and encrypted usage control  
25 policy data indicating the handling of the content data,

distributing the related produced key file from the management apparatus to the data processing apparatus, providing a content file storing the content data encrypted by using the content key data from the data providing apparatus to the data distribution apparatus, and distributing the provided content file from the data distribution apparatus to the data processing apparatus, and in the data processing apparatus, decrypting the content key data and the usage control policy data stored in the distributed key file and determining the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

Also, a data providing method of a 16th aspect of the present invention is a data providing method for providing content data from a data providing apparatus to a data distribution apparatus, distributing the content data from the data distribution apparatus to a data processing apparatus, and managing the data providing apparatus, the data distribution apparatus, and the data processing apparatus by a management apparatus, comprising the steps of, in the management apparatus, preparing a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, in the data providing

apparatus, providing a first module storing the content data encrypted by using the content key data and the key file received from the management apparatus to the data distribution apparatus, in the data distribution

5 apparatus, distributing a second module storing the provided content data and the key file to the data processing apparatus, and in the data processing apparatus, decrypting the content key data and the usage control policy data stored in the distributed second  
10 module and determining the handling of the content data stored in the distributed second module based on the related decrypted usage control policy data.

Also, a data providing method of a 17th aspect of the present invention is a data providing method for  
15 providing content data from a data providing apparatus to a data distribution apparatus, distributing the content data from the data distribution apparatus to a data processing apparatus, and managing the data providing apparatus, the data distribution apparatus, and the data  
20 processing apparatus by a management apparatus, comprising the steps of, in the management apparatus, preparing a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, in the data providing  
25 apparatus, individually distributing the content data

encrypted by using the content key data and the key file  
received from the management apparatus to the data  
distribution apparatus, in the data distribution  
apparatus, individually distributing the distributed  
5 content data and the key file to the data distribution  
apparatus, and in the data processing apparatus,  
decrypting the content key data and the usage control  
policy data stored in the distributed key file and  
determining the handling of the distributed content data  
10 based on the related decrypted usage control policy data.

Also, a data providing method of an 18th aspect of  
the present invention is a data providing method for  
distributing content data from a data providing apparatus  
to a data processing apparatus and managing the data  
15 providing apparatus and the data processing apparatus by  
a management apparatus, comprising the steps of, in the  
management apparatus, preparing a key file storing  
encrypted content key data and encrypted usage control  
policy data indicating the handling of the content data  
20 and distributing the related produced key file to the  
data processing apparatus, in the data providing  
apparatus, providing the content data encrypted by using  
the content key data to the data distribution apparatus,  
in the data distribution apparatus, distributing the  
25 provided content data to the data processing apparatus,

and in the data processing apparatus, decrypting the content key data and the usage control policy data stored in the distributed key file and determining the handling of the distributed content data based on the related  
5    decrypted usage control policy data.

Also, a data providing method of a 19th aspect of the present invention is a data providing method for providing content data from a data providing apparatus to a data distribution apparatus, distributing the content  
10    data from the data distribution apparatus to a data processing apparatus, and managing the data providing apparatus, the data distribution apparatus, and the data processing apparatus by a management apparatus, comprising the steps of, in the management apparatus,  
15    providing encrypted content key data and encrypted usage control policy data indicating the handling of the content data to the data providing apparatus, in the data providing apparatus, individually distributing the content data encrypted by using the content key data and  
20    the encrypted content key data and the encrypted usage control policy data which are received from the management apparatus to the data distribution apparatus, in the data distribution apparatus, individually distributing the distributed content data, the encrypted  
25    content key data, and the encrypted usage control policy



data to the data distribution apparatus, and in the data processing apparatus, decrypting the distributed content key data and the usage control policy data and determining the handling of the distributed content data based on the related decrypted usage control policy data.

Also, a data providing method of a 20th aspect of the present invention is a data providing method for providing content data from a data providing apparatus to a data distribution apparatus, distributing the content data from the data distribution apparatus to a data processing apparatus, and managing the data providing apparatus, the data distribution apparatus, and the data processing apparatus by a management apparatus, comprising the steps of, in the management apparatus, distributing encrypted content key data and encrypted usage control policy data indicating the handling of the content data to the data processing apparatus, in the data providing apparatus, distributing the content data encrypted by using the content key data to the data distribution apparatus, in the data distribution apparatus, distributing the provided content data to the data processing apparatus, and in the data processing apparatus, decrypting the distributed content key data and the usage control policy data and determining the handling of the distributed content data based on the

related decrypted usage control policy data.

Also, a data providing method of a 21st aspect of the present invention is a data providing method using a data providing apparatus, a data distribution apparatus, a management apparatus, and a data processing apparatus, wherein the data providing apparatus provides master source data of content to the management apparatus, the management apparatus manages the data providing apparatus, the data distribution apparatus, and the data processing apparatus, encrypts the provided master source data by using content key data to produce content data, produces a content file storing the related content data, produces a key file storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data, and provides the content file and the key file to the data distribution apparatus, the data distribution apparatus distributes the provided content file and the key file to the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key file and determines the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

Also, a data providing method of a 22nd aspect of

the present invention is a data providing method using a data providing apparatus, a data distribution apparatus, a management apparatus, and a data processing apparatus, wherein the data providing apparatus provides master

5 source data of content to the management apparatus, the management apparatus manages the data providing apparatus, the data distribution apparatus, and the data processing apparatus, encrypts the provided master source data by using content key data to produce content data,

10 produces a content file storing the related content data, produces a key file storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data, and provides the content file to the data distribution apparatus and

15 provides the key file to the data processing apparatus, the data distribution apparatus distributes the provided content file to the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the provided

20 key file and determines the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

Also, a data providing method of a 23rd aspect of the present invention is a data providing method using a

25 data providing apparatus, a data distribution apparatus,

a management apparatus, and a data processing apparatus,  
wherein the data providing apparatus provides a content  
file storing encrypted content data using content key  
data to the management apparatus, the management  
5 apparatus manages the data providing apparatus, the data  
distribution apparatus, and the data processing  
apparatus, produces a key file storing the encrypted  
content key data and encrypted usage control policy data  
indicating the handling of the content data, provides the  
10 content file provided from the data providing apparatus  
and the produced key file to the data distribution  
apparatus, the data distribution apparatus distributes  
the provided content file and the key file to the data  
processing apparatus, and the data processing apparatus  
15 decrypts the content key data and the usage control  
policy data stored in the distributed key file and  
determines the handling of the content data stored in the  
distributed content file based on the related decrypted  
usage control policy data.

20 Also, a data providing method of a 24th aspect of  
the present invention is a data providing method using a  
data providing apparatus, a data distribution apparatus,  
a management apparatus, and a data processing apparatus,  
wherein the data providing apparatus provides a content  
25 file storing encrypted content data using content key

data to the management apparatus, the management apparatus manages the data providing apparatus, the data distribution apparatus, and the data processing apparatus, produces a key file storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data, provides the content file provided from the data providing apparatus to the data distribution apparatus, and provides the produced key file to the data processing apparatus, the data distribution apparatus distributes the provided content file to the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the provided key file and determines the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

Also, a data providing method of a 25th aspect of the present invention is a data providing method using a data providing apparatus, a data distribution apparatus, a management apparatus, a database device, and a data processing apparatus, wherein the data providing apparatus encrypts content data by using content key data, produces a content file storing the related encrypted content data, and stores the related produced content file and a key file provided from the management

apparatus in the database device, the management  
apparatus produces a key file storing the encrypted  
content key data and encrypted usage control policy data  
indicating the handling of the content data and provides  
5 the related produced key file to the data providing  
apparatus, the data distribution apparatus distributes  
the content file and key file obtained from the database  
device to the data processing apparatus, and the data  
processing apparatus decrypts the content key data and  
10 the usage control policy data stored in the distributed  
key file and determines the handling of the content data  
stored in the distributed content file based on the  
related decrypted usage control policy data.

Also, a data providing method of a 26th aspect of  
15 the present invention is a data providing method using a  
data providing apparatus, a data distribution apparatus,  
a management apparatus, a database device, and a data  
processing apparatus, wherein the data providing  
apparatus encrypts content data by using content key  
20 data, produces a content file storing the related  
encrypted content data, and stores the related produced  
content file in the database device, the management  
apparatus produces a key file storing the encrypted  
content key data and encrypted usage control policy data  
25 indicating the handling of the content data and provides

the related produced key file to the data distribution apparatus, the data distribution apparatus distributes the content file obtained from the database device and the key file provided from the data distribution  
5 apparatus to the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key file and determines the handling of the content data stored in the distributed content file based on the  
10 related decrypted usage control policy data.

Also, a data providing method of a 27th aspect of the present invention is a data providing method using a data providing apparatus, a data distribution apparatus, a management apparatus, a database device, and a data  
15 processing apparatus, wherein the data providing apparatus encrypts content data by using content key data, produces a content file storing the related encrypted content data, and stores the related produced content file in the database device, the management  
20 apparatus produces a key file storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data and provides the related produced key file to the data processing apparatus, the data distribution apparatus distributes  
25 the content file obtained from the database device and

the key file provided from the data distribution apparatus to the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the provided key file and determines the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

Also, a data providing method of a 28th aspect of the present invention is a data providing method using a plurality of data providing apparatuses, a data distribution apparatus, a plurality of management apparatuses, a database device, and a data processing apparatus, wherein the data providing apparatuses encrypt content data by using content key data, produce content files storing the related encrypted content data, and store the related produced content files and key files provided from corresponding management apparatuses in the database device, the management apparatuses produce the key files storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data for the content data provided by corresponding data providing apparatuses and provide the related produced key files to corresponding data providing apparatuses, the data distribution apparatus distributes the content files and key files



obtained from the database device to the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key files and determines the handling  
5 of the content data stored in the distributed content files based on the related decrypted usage control policy data.

Also, a data providing method of a 29th aspect of the present invention is a data providing method using a  
10 plurality of data providing apparatuses, a data distribution apparatus, a plurality of management apparatuses, a database device, and a data processing apparatus, wherein the data providing apparatuses encrypt content data by using content key data, produce content  
15 files storing the related encrypted content data, and store the related produced content files in the database device, the management apparatuses produce the key files storing the encrypted content key data and encrypted usage control policy data indicating the handling of the  
20 content data for the content data provided by corresponding data providing apparatuses and provide the related produced key files to the data distribution apparatus, the data distribution apparatus distributes the content files obtained from the database device and  
25 the key files provided from the management apparatuses to

the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key files and determines the handling of the content data stored in the distributed content files based on the related decrypted usage control policy data.

Also, a data providing method of a 30th aspect of the present invention is a data providing method using a plurality of data providing apparatuses, a data distribution apparatus, a plurality of management apparatuses, a database device, and a data processing apparatus, wherein the data providing apparatuses encrypt content data by using content key data, produce content files storing the related encrypted content data, and store the related produced content files in the database device, the management apparatuses produce the key files storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data for the content data provided by corresponding data providing apparatuses and provide the related produced key files to the data processing apparatus, the data distribution apparatus distributes the content files obtained from the database device to the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage

control policy data stored in the provided key files and determines the handling of the content data stored in the distributed content files based on the related decrypted usage control policy data.

5       Also, a data providing method of a 31st aspect of the present invention is a data providing method using a plurality of data providing apparatuses, a data distribution apparatus, a plurality of management apparatuses, a database device, and a data processing  
10   apparatus, wherein the data providing apparatuses provide master sources of content data to corresponding management apparatuses and store content files and key files received from the related management apparatuses in the database, the management apparatuses encrypt the  
15   master sources received from corresponding data providing apparatuses by using content key data, produce content files storing the related encrypted content data, produce key files storing the encrypted content key data and encrypted usage control policy data indicating the  
20   handling of the content data for the content data provided by corresponding data providing apparatuses, and send the produced content files and the produced key files to corresponding data providing apparatuses, the data distribution apparatus distributes the content files  
25   and key files obtained from the database device to the

data processing apparatus, and the data processing  
apparatus decrypts the content key data and the usage  
control policy data stored in the distributed key files  
and determines the handling of the content data stored in  
5 the distributed content files based on the related  
decrypted usage control policy data.

Also, a data providing method of a 32nd aspect of  
the present invention is a data providing method using a  
plurality of data providing apparatuses, a data  
10 distribution apparatus, a plurality of management  
apparatuses, a database device, and a data processing  
apparatus, wherein the data providing apparatuses provide  
master sources of content data to corresponding  
management apparatuses and store content files received  
15 from the related management apparatuses in the database,  
the management apparatuses encrypt the master sources  
received from corresponding data providing apparatuses by  
using content key data, produce content files storing the  
related encrypted content data, send the related produced  
20 content files to the data providing apparatuses, produce  
key files storing the encrypted content key data and  
encrypted usage control policy data indicating the  
handling of the content data for the content data  
provided by corresponding data providing apparatuses, and  
25 send the related produced key files to corresponding data

distribution apparatus, the data distribution apparatus distributes the content files obtained from the database device and key files provided from the management apparatuses to the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key files and determines the handling of the content data stored in the distributed content files based on the related decrypted usage control policy data.

Also, a data providing method of a 33rd aspect of the present invention is a data providing method using a plurality of data providing apparatuses, a data distribution apparatus, a plurality of management apparatuses, a database device, and a data processing apparatus, wherein the data providing apparatuses provide master sources of content data to corresponding management apparatuses and store content files received from the related management apparatuses in the database, the management apparatuses encrypt the master sources received from corresponding data providing apparatuses by using content key data, produce content files storing the related encrypted content data, send the related produced content files to the data providing apparatuses, produce key files storing the encrypted content key data and encrypted usage control policy data indicating the

handling of the content data for the content data  
provided by corresponding data providing apparatuses, and  
provide the related produced key files to the data  
processing apparatus, the data distribution apparatus  
5 distributes the content files obtained from the database  
device to the data processing apparatus, and the data  
processing apparatus decrypts the content key data and  
the usage control policy data stored in the provided key  
files and determines the handling of the content data  
10 stored in the distributed content files based on the  
related decrypted usage control policy data.

Also, a data providing system of a 34th aspect of  
the present invention is a data providing system for  
distributing content data from a data providing apparatus  
15 to a data processing apparatus, wherein the data  
providing apparatus distributes a module storing the  
content data encrypted by using content key data, the  
encrypted content key data, and encrypted usage control  
policy data indicating the handling of the content data  
20 to the data processing apparatus by using a predetermined  
communication protocol in a format not depending upon the  
related communication protocol or by recording the same  
on a storage medium, and the data processing apparatus  
decrypts the content key data and the usage control  
25 policy data stored in the distributed module and

determines the handling of the content data based on the related decrypted usage control policy data.

The mode of operation of the data providing system of the 34th aspect of the present invention becomes as follows.

The module storing the content data encrypted by using the content key data, the encrypted content key data, and the encrypted usage control policy data indicating the handling of the content data is distributed from the data providing apparatus to the data processing apparatus.

At this time, the related module is distributed from the data providing apparatus to the data processing apparatus by using a predetermined communication protocol in a format not depending upon the related communication protocol or while being recorded on a storage medium.

Then, in the data processing apparatus, the content key data and the usage control policy data stored in the distributed module are decrypted, and the handling of the content data is determined based on the related decrypted usage control policy data.

In this way, by storing the usage control policy data indicating the handling of the related content data in the module storing the content data, in the data processing apparatus, it becomes possible to handle (use)

the content data based on the usage control policy data produced by the interested parties of the data providing apparatus.

Also, the module is distributed from the data  
5 providing apparatus to the data processing apparatus in the format not depending upon a predetermined communication protocol, so a compression method, encryption method, etc. of the content data stored in the module can be freely determined by the data providing  
10 apparatus.

Also, in the data providing system of the 34th aspect of the present invention, preferably the module further storing signature data for verifying a legitimacy of a producer and a transmitter of at least one data  
15 among the content data, the content key data, and the usage control policy data is distributed to the data processing apparatus.

Also, in the data providing system of the 34th aspect of the present invention, preferably the data  
20 providing apparatus distributes the module further storing at least one data between data for verifying if the related data is not tampered with and signature data for verifying if the related data was normally certified by a predetermined manager for at least one data among  
25 the content data, the content key data, and the usage



control policy data to the data processing apparatus.

Also, in the data providing system of the 34th aspect of the present invention, preferably the data processing apparatus determines a purchase form of the content data based on the usage control policy data, and where the content data is transferred to another data processing apparatus, the signature data indicating the legitimacy of the purchaser of the related content data and the signature data indicating the legitimacy of the transmitter of the related content data are made different.

A data providing system of 35th aspect of the present invention is a data providing system for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, wherein the management apparatus produces a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, the data providing apparatus distributes a module storing a content file storing the content data encrypted by using the content key data and the key file received from the management apparatus to the data processing apparatus by using a predetermined communication protocol in a format not

depending upon the related communication protocol or by  
recording the same on a storage medium, and the data  
processing apparatus decrypts the content key data and  
the usage control policy data stored in the distributed  
5 module and determines the handling of the content data  
based on the related decrypted usage control policy data.

The mode of operation of the data providing system  
of the 35th aspect of the present invention becomes as  
follows.

10 In the management apparatus, the key file storing  
the encrypted content key data and the encrypted usage  
control policy data indicating the handling of the  
content data is produced.

Then, the related produced key file is distributed  
15 from the management apparatus to the data providing  
apparatus.

Then, the module storing the content file storing  
the content data encrypted by using the content key data  
and the key file received from the management apparatus  
20 is distributed from the data providing apparatus to the  
data processing apparatus by using a predetermined  
communication protocol but in a format not depending upon  
the related communication protocol or while being  
recorded on a storage medium.

25 Then, in the data processing apparatus, the content

key data and the usage control policy data stored in the distributed module are decrypted, and the handling of the content data is determined based on the related decrypted usage control policy data.

5       Also, in the data providing system of the 35th aspect of the present invention, preferably the management apparatus produces signature data for verifying the legitimacy of the producer of the key file and produces the key file further storing the related  
10   signature data.

      Also, in the data providing system of the 35th aspect of the present invention, preferably the data providing apparatus produces the content key data and the usage control policy data and transmits the same to the  
15   management apparatus, and the management apparatus produces the key file based on the received content key data and usage control policy data and registers the related produced key file.

      Also, a data providing apparatus of the present  
20   invention is a data providing apparatus which is managed by a management apparatus and distributes content data to a data processing apparatus, receiving a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data  
25   from the management apparatus and distributing a module

storing a content file storing the content data encrypted by using the content key data and the key file received from the management apparatus to the data processing apparatus.

5           Also, a data processing apparatus of the present invention is a data processing apparatus managed by a management apparatus and utilizing content data, receiving a module containing a key file storing encrypted content key data and encrypted usage control  
10   policy data indicating the handling of the content data and a content file storing the content data encrypted by using the content key data, determining at least one between a purchase form and an usage form of the content data based on the usage control policy data, and  
15   transmitting a log data indicating the log of the determined at least one of the related purchase form and usage form to the management apparatus.

          Also, a data providing system of a 36th aspect of the present invention is a data providing system for  
20   distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, wherein the management apparatus produces a key file storing encrypted content key data  
25   and encrypted usage control policy data indicating the

handling of the content data, the data providing apparatus distributes a module storing a content file containing the content data encrypted by using the content key data and the key file received from the management apparatus to the data processing apparatus by using a predetermined communication protocol in a format not depending upon the related communication protocol or recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed module and determines the handling of the content data based on the related decrypted usage control policy data.

The mode of operation of the data providing system of the 36th aspect of the present invention becomes as follows.

In the management apparatus, the key file storing the encrypted content key data and the encrypted usage control policy data indicating the handling of the content data is produced, and the related key file is sent to the data providing apparatus.

Then, the module storing the content file containing the content data encrypted by using the content key data and the key file received from the management apparatus is distributed from the data providing apparatus to the data processing apparatus by using a predetermined

communication protocol in a format not depending upon the related communication protocol or while being recorded on a storage medium.

Then, in the data processing apparatus, the content  
5 key data and the usage control policy data stored in the distributed module are decrypted, and the handling of the content data is determined based on the related decrypted usage control policy data.

Also, a data providing system of a 37th aspect of  
10 the present invention is a data providing system for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, wherein the management apparatus  
15 produces a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, the data providing apparatus individually distributes a content file storing the content data encrypted by using the content key data  
20 and the key file received from the management apparatus to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or by recording the same on a storage medium, and the data processing  
25 apparatus decrypts the content key data and the usage

control policy data stored in the distributed key file and determines the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

5           The mode of operation of the data providing system of the 37th aspect of the present invention becomes as follows. In the management apparatus, the key file storing the encrypted content key data and the encrypted usage control policy data indicating the handling of the  
10   content data is produced, and the related key file is sent to the data providing apparatus.

          Then, in the data processing apparatus, the content file storing the content data encrypted by using the content key data and the key file received from the  
15   management apparatus are individually distributed to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or while being recorded on a storage medium.

20           Then, in the data processing apparatus, the content key data and the usage control policy data stored in the distributed key file are decrypted, and the handling of the content data stored in the distributed content file is determined based on the related decrypted usage  
25   control policy data.

Also, a data providing system of a 38th aspect of the present invention is a data providing system for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, wherein the management apparatus produces a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data and distributes the related produced key file to the data processing apparatus, the data providing apparatus distributes a content file storing the content data encrypted by using the content key data to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key file and determines the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

Below, an explanation will be made of the mode of operation of the data providing system of the 38th aspect of the present invention.

In the management apparatus, the key file storing



the encrypted content key data and the encrypted usage control policy data indicating the handling of the content data is produced.

The related produced key file is distributed from  
5 the management apparatus to the data processing apparatus.

Also, the content file storing the content data encrypted by using the content key data is distributed from the data providing apparatus to the data processing  
10 apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or while being recorded on a storage medium.

Then, in the data processing apparatus, the content  
15 key data and the usage control policy data stored in the distributed key file are decrypted, and the handling of the content data stored in the distributed content file is determined based on the related decrypted usage control policy data.

Also, a data providing system of a 39th aspect of  
20 the present invention is a data providing system for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by  
25 a management apparatus, wherein the management apparatus

produces a key file storing encrypted content key data  
and encrypted usage control policy data indicating the  
handling of the content data, the data providing  
apparatus distributes a module storing the content data  
5 encrypted by using the content key data and the key file  
received from the management apparatus to the data  
processing apparatus by using a predetermined  
communication protocol but in a format not depending upon  
the related communication protocol or recording the same  
10 on a storage medium, and the data processing apparatus  
decrypts the content key data and the usage control  
policy data stored in the distributed module and  
determines the handling of the content data based on the  
related decrypted usage control policy data.

15 Below, an explanation will be made of the mode of  
operation of the data providing system of the 39th aspect  
of the present invention.

In the management apparatus, the key file storing  
the encrypted content key data and the encrypted usage  
20 control policy data indicating the handling of the  
content data is produced, and the related key file is  
sent to the data providing apparatus.

Then, the module storing the content data encrypted  
by using the content key data and the key file received  
25 from the management apparatus is distributed from the

data providing apparatus to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or while being recorded on a storage medium.

5           Then, in the data processing apparatus, the content key data and the usage control policy data stored in the distributed module are decrypted, and the handling of the content data is determined based on the related decrypted usage control policy data.

10           Also, a data providing system of a 40th aspect of the present invention is a data providing system for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by  
15           a management apparatus, wherein the management apparatus produces a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, the data providing apparatus individually distributes the content data  
20           encrypted by using the content key data and the key file received from the management apparatus to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same  
25           on a storage medium, and the data processing apparatus

decrypts the content key data and the usage control policy data stored in the distributed key file and determines the handling of the distributed content data based on the related decrypted usage control policy data.

5       Below, an explanation will be made of the mode of operation of the data providing system of the 40th aspect of the present invention.

10       In the management apparatus, the key file storing the encrypted content key data and the encrypted usage control policy data indicating the handling of the content data is produced, and the related key file is sent to the data providing apparatus.

15       Then, the content data encrypted by using the content key data and the key file received from the management apparatus are individually distributed from the data providing apparatus to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or while being recorded on a storage medium.

20       Then, in the data processing apparatus, the content key data and the usage control policy data stored in the distributed key file are decrypted, and the handling of the distributed content data is determined based on the related decrypted usage control policy data.

Also, a data providing system of a 41st aspect of the present invention is a data providing system for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, wherein the management apparatus produces a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data and distributes the related produced key file to the data processing apparatus, the data providing apparatus distributes the content data encrypted by using the content key data to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key file and determines the handling of the distributed content data based on the related decrypted usage control policy data.

Below, an explanation will be made of the mode of operation of the data providing system of the 41st aspect of the present invention.

In the management apparatus, the key file storing the encrypted content key data and the encrypted usage

control policy data indicating the handling of the content data is produced, and the related produced key file is distributed to the data processing apparatus.

Also, the content data encrypted by using the  
5 content key data is distributed from the data providing apparatus to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or while being recorded on a storage medium.

10 Then, in the data processing apparatus, the content key data and the usage control policy data stored in the distributed key file are decrypted, and the handling of the distributed content data is determined based on the related decrypted usage control policy data.

15 Also, a data providing system of a 42nd aspect of the present invention is a data providing system for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by  
20 a management apparatus, wherein the management apparatus produces encrypted content key data and encrypted usage control policy data indicating the handling of the content data, the data providing apparatus individually distributes the content data encrypted by using the  
25 content key data and the encrypted content key data and

the encrypted usage control policy data received from the management apparatus to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication  
5 protocol or recording the same on a storage medium, and the data processing apparatus decrypts the distributed content key data and the usage control policy data and determines the handling of the content data stored in the distributed content file based on the related decrypted  
10 usage control policy data.

Below, an explanation will be made of the mode of operation of the data providing system of the 42nd aspect of the present invention.

In the management apparatus, the encrypted content  
15 key data and the encrypted usage control policy data indicating the handling of the content data are produced and are sent to the data providing apparatus.

Then, the content data encrypted by using the content key data and the encrypted content key data and  
20 the encrypted usage control policy data received from the management apparatus are individually distributed from the data providing apparatus to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related  
25 communication protocol or while being recorded on a

storage medium.

Then, in the data processing apparatus, the distributed content key data and the usage control policy data are decrypted, and the handling of the content data  
5 stored in the distributed content file is determined based on the related decrypted usage control policy data.

Also, a data providing system of a 43rd aspect of the present invention is a data providing system for distributing content data from a data providing apparatus  
10 to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, wherein the management apparatus produces encrypted content key data and encrypted usage control policy data indicating the handling of the  
15 content data and distributes the same to the data processing apparatus, the data providing apparatus distributes the content data encrypted by using the content key data to the data processing apparatus by using a predetermined communication protocol but in a  
20 format not depending upon the related communication protocol or recording the same on a storage medium, and the data processing apparatus decrypts the distributed content key data and the usage control policy data and determines the handling of the distributed content data  
25 based on the related decrypted usage control policy data.



Below, an explanation will be made of the mode of operation of the data providing system of the 43rd aspect of the present invention.

In the management apparatus, the encrypted content  
5 key data and the encrypted usage control policy data indicating the handling of the content data are produced and are distributed to the data processing apparatus.

Then, the content data encrypted by using the content key data is distributed from the data providing  
10 apparatus to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or while being recorded on a storage medium.

Then, in the data processing apparatus, the  
15 distributed content key data and the usage control policy data are decrypted, and the handling of the distribution the content data is determined based on the related decrypted usage control policy data.

Also, a data providing system of a 44th aspect of  
20 the present invention is a data providing system having a data providing apparatus, a data distribution apparatus, and a data processing apparatus, wherein the data providing apparatus provides a first module storing content data encrypted by using content key data, the  
25 encrypted content key data, and encrypted usage control

policy data indicating the handling of the content data  
to the data distribution apparatus, the data distribution  
apparatus distributes a second module storing the  
encrypted content data, content key data, and the usage  
5 control policy data stored in the provided first module  
to the data processing apparatus by using a predetermined  
communication protocol but in a format not depending upon  
the related communication protocol or by recording the  
same on a storage medium, and the data processing  
10 apparatus decrypts the content key data and the usage  
control policy data stored in the distributed second  
module and determines the handling of the content data  
based on the related decrypted usage control policy data.

Below, an explanation will be made of the mode of  
15 operation of the data providing system of the 44th aspect  
of the present invention.

The first module storing the content data encrypted  
by using the content key data, the encrypted content key  
data, and the encrypted usage control policy data  
20 indicating the handling of the content data is provided  
from the data providing apparatus to the data  
distribution apparatus by for example using a  
predetermined communication protocol but in a format not  
depending upon the related communication protocol or  
25 while being recorded on a storage medium.

Next, the second module storing the encrypted content data, content key data, and the usage control policy data stored in the provided first module is distributed from the data distribution apparatus to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or while being recorded on a storage medium.

Then, in the data processing apparatus, the content key data and the usage control policy data stored in the distributed second module are decrypted, and the handling of the content data is determined based on the related decrypted usage control policy data.

In this way, by storing the usage control policy data indicating the handling of the related content data in the first module and second module storing the content data, in the data processing apparatus, it becomes possible to have the data processing apparatus perform the handling (usage) of the content data based on the usage control policy data produced by the interested parties of the data providing apparatus.

Also, the second module is distributed from the data distribution apparatus to the data processing apparatus in a format not depending upon on a predetermined communication protocol, so the compression method and

encryption method etc. of the content data stored in the second module can be freely determined by the data providing apparatus.

A data providing system of a 45th aspect of the present invention is a data providing system for providing content data from a data providing apparatus to a data distribution apparatus, distributing the content data from the data distribution apparatus to a data processing apparatus, and managing the data providing apparatus, the data distribution apparatus, and the data processing apparatus by a management apparatus, wherein the management apparatus produces a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, the data providing apparatus provides a first module storing a content file storing the content data encrypted by using the content key data and the key file received from the management apparatus to the data distribution apparatus, the data distribution apparatus distributes a second module storing the provided content file and the key file to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and the data processing apparatus decrypts the content key data and

the usage control policy data stored in the distributed second module and determines the handling of the content data stored in the distributed second module based on the related decrypted usage control policy data.

5           Below, an explanation will be made of the mode of operation of the data providing system of the 45th aspect of the present invention.

10           In the management apparatus, the key file storing the encrypted content key data and the encrypted usage control policy data indicating the handling of the content data is produced, and the related key file is sent to the data providing apparatus.

15           Then, the first module storing the content file storing the content data encrypted by using the content key data and the key file received from the management apparatus is provided from the data providing apparatus to the data distribution apparatus.

20           Then, the second module storing the provided content file and the key file is distributed from the data distribution apparatus to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or while being recorded on a storage medium.

25           Then, in the data processing apparatus, the content key data and the usage control policy data stored in the

distributed second module are decrypted, and the handling of the content data stored in the distributed second module is determined based on the related decrypted usage control policy data.

5           A data providing system of a 46th aspect of the present invention is a data providing system for providing content data from a data providing apparatus to a data distribution apparatus, distributing the content data from the data distribution apparatus to a data  
10   processing apparatus, and managing the data providing apparatus, the data distribution apparatus, and the data processing apparatus by a management apparatus, wherein the management apparatus produces a key file storing encrypted content key data and encrypted usage control  
15   policy data indicating the handling of the content data, the data providing apparatus provides a first module storing a content file containing the content data encrypted by using the content key data and a key file received from the management apparatus to the data  
20   distribution apparatus, the data distribution apparatus distributes a second module storing the provided content file to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or  
25   recording the same on a storage medium, and the data

processing apparatus decrypts the content key data and  
the usage control policy data stored in the distributed  
second module and determines the handling of the content  
data stored in the distributed second module based on the  
5 related decrypted usage control policy data.

Also, a data providing system of a 47th aspect of  
the present invention is a data providing system for  
providing content data from a data providing apparatus to  
a first data distribution apparatus and a second data  
10 distribution apparatus, distributing the content data  
from the first data distribution apparatus and the second  
data distribution apparatus to a data processing  
apparatus, and managing the data providing apparatus, the  
first data distribution apparatus, the second data  
15 distribution apparatus, and the data processing apparatus  
by a management apparatus, wherein the management  
apparatus produces a key file storing encrypted content  
key data and encrypted usage control policy data  
indicating the handling of the content data, the data  
20 providing apparatus provides a first module storing a  
content file storing the content data encrypted by using  
the content key data and the key file received from the  
management apparatus to the first data distribution  
apparatus and the second data distribution apparatus, the  
25 first data distribution apparatus distributes a second

module storing the provided content file and the key file  
to the data processing apparatus, the second data  
distribution apparatus distributes a third module storing  
the provided content file and the key file to the data  
5 processing apparatus, and the data processing apparatus  
decrypts the content key data and the usage control  
policy data stored in the distributed second module and  
the third module and determines the handling of the  
content data based on the related decrypted usage control  
10 policy data.

Also, a data providing system of a 48th aspect of  
the present invention is a data providing system for  
providing first content data from a first data providing  
apparatus to a data distribution apparatus, providing  
15 second content data from a second data providing  
apparatus to the data distribution apparatus,  
distributing the content data from the data distribution  
apparatus to a data processing apparatus, and managing  
the first data providing apparatus, the second data  
20 providing apparatus, the data distribution apparatus, and  
the data processing apparatus by a management apparatus,  
wherein the management apparatus produces a first key  
file storing an encrypted first content key data and an  
encrypted first usage control policy data indicating the  
25 handling of the first content data and a second key file



storing an encrypted second content key data and an encrypted second usage control policy data indicating the handling of the second content data, the first data providing apparatus provides a first module storing a  
5 first content file storing the first content data encrypted by using the first content key data and the first key file received from the management apparatus to the data distribution apparatus, the second data providing apparatus provides a second module storing a  
10 second content file storing the second content data encrypted by using the second content key data and the second key file received from the management apparatus to the data distribution apparatus, the data distribution apparatus distributes a third module storing the provided  
15 first content file, the first key file, the second content file, and the second key file to the data processing apparatus, and the data processing apparatus decrypts the first content key data, the second content key data, the first usage control policy data, and the  
20 second usage control policy data stored in the distributed third module, determines the handling of the first content data based on the related decrypted first usage control policy data, and determines the handling of the second content data based on the related decrypted  
25 second usage control policy data.

Also, a data providing system of a 49th aspect of the present invention is a data providing system for providing content data from a data providing apparatus to a data distribution apparatus, distributing the content data from the data distribution apparatus to a data processing apparatus, and managing the data providing apparatus, the data distribution apparatus, and the data processing apparatus by a management apparatus, wherein the management apparatus produces a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, the data providing apparatus individually distributes a content file storing the content data encrypted by using the content key data and the key file received from the management apparatus to the data distribution apparatus, the data distribution apparatus individually distributes the distributed content file and the key file to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or by recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key file and determines the handling of the content data stored in the distributed content file based on the related

decrypted usage control policy data.

Also, a data providing system of a 50th aspect of the present invention is a data providing system for providing content data from a data providing apparatus to  
5 a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, wherein the management apparatus produces a key file storing encrypted content key data and encrypted usage control policy data indicating the  
10 handling of the content data and distributes the related produced key file to the data processing apparatus, the data providing apparatus distributes a content file storing the content data encrypted by using the content key data to the data distribution apparatus, the data  
15 distribution apparatus distributes the provided content file to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or by recording the same on a storage medium, and the data  
20 processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key file and determines the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

25 Also, a data providing system of a 51st aspect of

the present invention is a data providing system for providing content data from a data providing apparatus to a data distribution apparatus, distributing the content data from the data distribution apparatus to a data processing apparatus, and managing the data providing apparatus, the data distribution apparatus, and the data processing apparatus by a management apparatus, wherein the management apparatus produces a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, the data providing apparatus provides a first module storing the content data encrypted by using the content key data and the key file received from the management apparatus to the data distribution apparatus, the data distribution apparatus distributes a second module storing the provided content data and the key file to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or by recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed second module and determines the handling of the content data stored in the distributed second module based on the related decrypted usage control policy data.

Also, a data providing system of a 52nd aspect of the present invention is a data providing system for providing content data from a data providing apparatus to a data distribution apparatus, distributing the content data from the data distribution apparatus to a data processing apparatus, and managing the data providing apparatus, the data distribution apparatus, and the data processing apparatus by a management apparatus, wherein the management apparatus produces a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, the data providing apparatus individually distributes the content data encrypted by using the content key data and the key file received from the management apparatus to the data distribution apparatus, the data distribution apparatus individually distributes the distributed content data and the key file to the data distribution apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or by recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key file and determines the handling of the distributed content data based on the related decrypted usage control policy data.

Also, a data providing system of a 53rd aspect of the present invention is a data providing system for providing content data from a data providing apparatus to a data processing apparatus, and managing the data

5 providing apparatus and the data processing apparatus by a management apparatus, wherein the management apparatus produces a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data and distributes the related

10 produced key file to the data processing apparatus, the data providing apparatus distributes the content data encrypted by using the content key data to the data distribution apparatus, the data distribution apparatus distributes the provided content data to the data

15 processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or by recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage

20 control policy data stored in the distributed key file and determines the handling of the distributed content data based on the related decrypted usage control policy data.

Also, a data providing system of a 54th aspect of

25 the present invention is a data providing system for

providing content data from a data providing apparatus to  
a data distribution apparatus, distributing the content  
data from the data distribution apparatus to a data  
processing apparatus, and managing the data providing  
5 apparatus, the data distribution apparatus, and the data  
processing apparatus by a management apparatus, wherein  
the management apparatus provides encrypted content key  
data and encrypted usage control policy data indicating  
the handling of the content data to the data providing  
10 apparatus, the data providing apparatus individually  
distributes the content data encrypted by using the  
content key data and the encrypted content key data and  
the encrypted usage control policy data received from the  
management apparatus to the data distribution apparatus,  
15 the data distribution apparatus distributes the  
distributed content data, the encrypted content key data,  
and the encrypted usage control policy data to the data  
distribution apparatus by using a predetermined  
communication protocol but in a format not depending upon  
20 the related communication protocol or recording the same  
on a storage medium, and the data processing apparatus  
decrypts the distributed content key data and the usage  
control policy data and determines the handling of the  
distributed content data based on the related decrypted  
25 usage control policy data.

Also, a data providing system of a 55th aspect of the present invention is a data providing system for providing content data from a data providing apparatus to a data distribution apparatus, distributing the content data from the data distribution apparatus to a data processing apparatus, and managing the data providing apparatus, the data distribution apparatus, and the data processing apparatus by a management apparatus, wherein the management apparatus provides encrypted content key data and encrypted usage control policy data indicating the handling of the content data to the data processing apparatus, the data providing apparatus provides the content data encrypted by using the content key data to the data distribution apparatus, the data distribution apparatus distributes the distributed provided content data to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and the data processing apparatus decrypts the distributed content key data and the usage control policy data and determines the handling of the distributed content data based on the related decrypted usage control policy data.

Also, a data providing system of a 56th aspect of the present invention is a data providing system having a



data providing apparatus, a data distribution apparatus,  
a management apparatus, and a data processing apparatus,  
wherein the data providing apparatus provides master  
source data of content to the management apparatus, the  
5 management apparatus manages the data providing  
apparatus, the data distribution apparatus, and the data  
processing apparatus, encrypts the provided master source  
data by using content key data to produce content data,  
produces a content file storing the related content data,  
10 produces a key file storing the encrypted content key  
data and encrypted usage control policy data indicating  
the handling of the content data, and provides the  
content file and the key file to the data distribution  
apparatus, the data distribution apparatus distributes  
15 the provided content file and the key file to the data  
processing apparatus by using a predetermined  
communication protocol but in a format not depending upon  
the related communication protocol or recording the same  
on a storage medium, and the data processing apparatus  
20 decrypts the content key data and the usage control  
policy data stored in the distributed key file and  
determines the handling of the content data stored in the  
distributed content file based on the related decrypted  
usage control policy data.

25 Also, in the data providing system of the 56th

aspect of the present invention, preferably the management apparatus produces a first module storing the content file and the key file and provides the related first module to the data distribution apparatus, and the data distribution apparatus produces a second module storing the content file and the key file stored in the first module and distributes the related second module to the data processing apparatus.

Also, in the data providing system of the 56th aspect of the present invention, preferably the management apparatus has at least one database among a database for storing and managing the content file, a database for storing and managing the key file, and a database for storing and managing the usage control policy data and centrally manages at least one among the content file, the key file, and the usage control policy data by using a content identifier uniquely allocated to the content data.

Also, a data providing system of a 57th aspect of the present invention is a data providing system having a data providing apparatus, a data distribution apparatus, a management apparatus, and a data processing apparatus, wherein the data providing apparatus provides master source data of content to the management apparatus, the management apparatus manages the data providing

apparatus, the data distribution apparatus, and the data processing apparatus, encrypts the provided master source data by using content key data to produce content data, produces a content file storing the related content data, produces a key file storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data, and provides the content file to the data distribution apparatus and provides the key file to the data processing apparatus, the data distribution apparatus distributes the provided content file to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the provided key file and determines the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

Also, a data providing system of a 58th aspect of the present invention is a data providing system having a data providing apparatus, a data distribution apparatus, a management apparatus, and a data processing apparatus, wherein the data providing apparatus provides a content file storing encrypted content data using content key

data to the management apparatus, the management apparatus manages the data providing apparatus, the data distribution apparatus, and the data processing apparatus, produces a key file storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data, and provides the content file provided from the data providing apparatus and the produced key file to the data distribution apparatus, the data distribution apparatus distributes the provided content file and the key file to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or by recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key file and determines the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

Also, a data providing system of a 59th aspect of the present invention is a data providing system having a data providing apparatus, a data distribution apparatus, a management apparatus, and a data processing apparatus, wherein the data providing apparatus provides a content file storing encrypted content data using content key

data to the management apparatus, the management apparatus manages the data providing apparatus, the data distribution apparatus, and the data processing apparatus, produces a key file storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data, provides the content file provided from the data providing apparatus to the data distribution apparatus, and provides the produced key file to the data processing apparatus, the data distribution apparatus distributes the provided content file to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or by recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the provided key file and determines the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

Also, a data providing system of a 60th aspect of the present invention is a data providing system having a data providing apparatus, a data distribution apparatus, a management apparatus, a database device, and a data processing apparatus, wherein the data providing apparatus encrypts content data by using content key

data, produces a content file storing the related encrypted content data, and stores the related produced content file and a key file provided from the management apparatus in the database device, the management

5 apparatus produces a key file storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data and provides the related produced key file to the data providing apparatus, the data distribution apparatus distributes  
10 the content file and key file obtained from the database device to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and the data  
15 processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key file and determines the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

20 Also, a data providing system of a 61st aspect of the present invention is a data providing system having a data providing apparatus, a data distribution apparatus, a management apparatus, a database device, and a data processing apparatus, wherein the data providing  
25 apparatus encrypts content data by using content key

data, produces a content file storing the related encrypted content data, and stores the related produced content file in the database device, the management apparatus produces a key file storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data and provides the related produced key file to the data providing apparatus, the data distribution apparatus distributes the content file obtained from the database device and the key file provided from the data distribution apparatus to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key file and determines the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

Also, a data providing system of a 62nd aspect of the present invention is a data providing system having a data providing apparatus, a data distribution apparatus, a management apparatus, a database device, and a data processing apparatus, wherein the data providing apparatus encrypts content data by using content key

data, produces a content file storing the related encrypted content data, and stores the related produced content file in the database device, the management apparatus produces a key file storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data and provides the related produced key file to the data processing apparatus, the data distribution apparatus distributes the content file obtained from the database device to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the provided key file and determines the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

Also, a data providing system of a 63rd aspect of the present invention is a data providing system having a plurality of data providing apparatuses, a data distribution apparatus, a plurality of management apparatuses, a database device, and a data processing apparatus, wherein the data providing apparatuses encrypt content data by using content key data, produce content



files storing the related encrypted content data, and  
store the related produced content files and key files  
provided from corresponding management apparatuses in the  
database device, the management apparatuses produce key  
5 files storing the encrypted content key data and  
encrypted usage control policy data indicating the  
handling of the content data for the content data  
provided by corresponding data providing apparatuses and  
provide the related produced key files to corresponding  
10 data providing apparatuses, the data distribution  
apparatus distributes the content files and key files  
obtained from the database device to the data processing  
apparatus by using a predetermined communication protocol  
but in a format not depending upon the related  
15 communication protocol or recording the same on a storage  
medium, and the data processing apparatus decrypts the  
content key data and the usage control policy data stored  
in the distributed key files and determines the handling  
of the content data stored in the distributed content  
20 files based on the related decrypted usage control policy  
data.

Also, a data providing system of a 64th aspect of  
the present invention is a data providing system having a  
plurality of data providing apparatuses, a data  
25 distribution apparatus, a plurality of management

apparatuses, a database device, and a data processing apparatus, wherein the data providing apparatuses encrypt content data by using content key data, produce content files storing the related encrypted content data, and

5 store the related produced content files in the database device, the management apparatuses produce key files storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data for the content data provided by

10 corresponding data providing apparatuses and provide the related produced key files to the data distribution apparatus, the data distribution apparatus distributes the content files obtained from the database device and the key files provided from the management apparatuses to

15 the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control

20 policy data stored in the distributed key files and determines the handling of the content data stored in the distributed content files based on the related decrypted usage control policy data.

Also, a data providing system of a 65th aspect of

25 the present invention is a data providing system having a

plurality of data providing apparatuses, a data distribution apparatus, a plurality of management apparatuses, a database device, and a data processing apparatus, wherein the data providing apparatuses encrypt  
5 content data by using content key data, produce content files storing the related encrypted content data, and store the related produced content files in the database device, the management apparatuses produce key files storing the encrypted content key data and encrypted  
10 usage control policy data indicating the handling of the content data for the content data provided by corresponding data providing apparatuses and provide the related produced key files to the data processing apparatus, the data distribution apparatus distributes  
15 the content files obtained from the database device to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and the data processing apparatus  
20 decrypts the content key data and the usage control policy data stored in the provided key files and determines the handling of the content data stored in the distributed content files based on the related decrypted usage control policy data.

25       Also, a data providing system of a 66th aspect of

the present invention is a data providing system having a plurality of data providing apparatuses, a data distribution apparatus, a plurality of management apparatuses, a database device, and a data processing apparatus, wherein the data providing apparatuses provide master sources of content data to corresponding management apparatuses and store content files and key files received from the related management apparatuses in the database, the management apparatuses encrypt the master sources received from corresponding data providing apparatuses by using content key data, produce content files storing the related encrypted content data, produce key files storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data for the content data provided by corresponding data providing apparatuses, and send the produced content files and the produced key files to corresponding data providing apparatuses, the data distribution apparatus distributes the content files and key files obtained from the database device to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or by recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage

control policy data stored in the distributed key files and determines the handling of the content data stored in the distributed content files based on the related decrypted usage control policy data.

5           Also, a data providing system of a 67th aspect of the present invention is a data providing system having a plurality of data providing apparatuses, a data distribution apparatus, a plurality of management apparatuses, a database device, and a data processing  
10   apparatus, wherein the data providing apparatuses provide master sources of content data to corresponding management apparatuses and store content files received from the related management apparatuses in the database, the management apparatuses encrypt the master sources  
15   received from corresponding data providing apparatuses by using content key data, produce content files storing the related encrypted content data, send the related produced content files to the data providing apparatuses, produce key files storing the encrypted content key data and  
20   encrypted usage control policy data indicating the handling of the content data for the content data provided by corresponding data providing apparatuses, and send the related produced key files provided from the management apparatuses to corresponding data distribution  
25   apparatus, the data distribution apparatus distributes

the content files obtained from the database device and key files provided from the management apparatuses to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon  
5 the related communication protocol or by recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key files and determines the handling of the content data stored in  
10 the distributed content files based on the related decrypted usage control policy data.

Also, a data providing system of a 68th aspect of the present invention is a data providing system having a plurality of data providing apparatuses, a data  
15 distribution apparatus, a plurality of management apparatuses, a database device, and a data processing apparatus, wherein the data providing apparatuses provide master sources of content data to corresponding management apparatuses and store content files received  
20 from the related management apparatuses in the database, the management apparatuses encrypt the master sources received from corresponding data providing apparatuses by using content key data, produce content files storing the related encrypted content data, send the related produced  
25 content files to the data providing apparatuses, produce

key files storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data for the content data provided by corresponding data providing apparatuses, and

5 send the related produced key files to the data processing apparatus, the data distribution apparatus distributes the content files obtained from the database device to the data processing apparatus by using a predetermined communication protocol but in a format not

10 depending upon the related communication protocol or by recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key files and determines the handling of the content data

15 stored in the provided content files based on the related decrypted usage control policy data.

Also, a data providing system of a 69th aspect of the present invention is a data providing system having a data providing apparatus, a data distribution apparatus,

20 and a data processing apparatus, wherein the data providing apparatus provides a first module storing content data encrypted by using content key data, the encrypted content key data, and encrypted usage control policy data indicating the handling of the content data

25 to the data distribution apparatus, performs charge

processing in units of the content data based on log data  
received from the data processing apparatus, and performs  
a profit distribution processing for distributing the  
profit paid by interested parties of the data processing  
5 apparatus to interested parties of the related data  
providing apparatus and interested parties of the data  
distribution apparatus, the data distribution apparatus  
distributes a second module storing the encrypted content  
data, content key data, and usage control policy data  
10 stored in the provided first module to the data  
processing apparatus by using a predetermined  
communication protocol but in a format not depending upon  
the related communication protocol or by recording the  
same on a storage medium, and the data processing  
15 apparatus decrypts the content key data and the usage  
control policy data stored in the distributed module,  
determines the handling of the content data based on the  
related decrypted usage control policy data, produces the  
log data for the handling of the related content data,  
20 and sends the related log data to the data providing  
apparatus.

Also, a data providing system of a 70th aspect of  
the present invention is a data providing system having a  
data providing apparatus, a data distribution apparatus,  
25 and a management apparatus, wherein the data providing



apparatus provides content data, the data distribution apparatus distributes the content file provided from the data providing apparatus or a content file in accordance with the content data provided by the data providing apparatus provided from the management apparatus to the data processing apparatus, and the data processing apparatus decrypts the usage control policy data stored in a key file received from the data distribution apparatus or the management apparatus, determines the handling of the content data stored in the content file received from the data distribution apparatus or the management apparatus based on the related decrypted usage control policy data, and further distributes the content file and key file received from the data distribution apparatus or the management apparatus to the other data processing apparatus.

Also, a data providing method of a 34th aspect of the present invention is a data providing method for distributing content data from a data providing apparatus to a data processing apparatus, comprising the steps of distributing a module storing the content data encrypted by using content key data, the encrypted content key data, and encrypted usage control policy data indicating the handling of the content data from the data providing apparatus to the data processing apparatus by using a

predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and in the data processing apparatus, decrypting the content key data and  
5 the usage control policy data stored in the distributed module and determining the handling of the content data based on the related decrypted usage control policy data.

Also, a data providing method of a 35h aspect of the present invention is a data providing method for  
10 distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, comprising the steps of, in the management apparatus, preparing a key file storing  
15 encrypted content key data and encrypted usage control policy data indicating the handling of the content data, distributing the produced key file from the management apparatus to the data providing apparatus, and  
distributing a module storing a content file storing the  
20 content data encrypted by using the content key data and the key file distributed from the management apparatus from the data providing apparatus to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related  
25 communication protocol or recording the same on a storage

medium, and in the data processing apparatus, decrypting the content key data and the usage control policy data stored in the distributed module and determining the handling of the content data based on the related  
5 decrypted usage control policy data.

Also, a data providing method of a 36th aspect of the present invention is a data providing method for distributing content data from a data providing apparatus to a data processing apparatus and managing the data  
10 providing apparatus and the data processing apparatus by a management apparatus, comprising the steps of, in the management apparatus, preparing a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data,  
15 in the data providing apparatus, distributing a module storing a content file containing the content data encrypted by using the content key data and a key file received from the management apparatus to the data processing apparatus by using a predetermined  
20 communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and in the data processing apparatus, decrypting the content key data and the usage control policy data stored in the distributed module and  
25 determining the handling of the content data based on the

related decrypted usage control policy data.

Also, a data providing method of a 37th aspect of the present invention is a data providing method for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, comprising the steps of, in the management apparatus, preparing a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, distributing the related produced key file from the management apparatus to the data providing apparatus, and individually distributing a content file storing the content data encrypted by using the content key data and the key file distributed from the management apparatus from the data providing apparatus to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and in the data processing apparatus, decrypting the content key data and the usage control policy data stored in the distributed key file and determining the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

Also, a data providing method of a 38th aspect of the present invention is a data providing method for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, comprising the steps of, in the management apparatus, preparing a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, distributing the related produced key file from the management apparatus to the data processing apparatus, and distributing a content file storing the content data encrypted by using the content key data from the data providing apparatus to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and in the data processing apparatus, decrypting the content key data and the usage control policy data stored in the distributed key file and determining the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

Also, a data providing method of a 39th aspect of the present invention is a data providing method for distributing content data from a data providing apparatus

to a data processing apparatus and managing the data  
providing apparatus and the data processing apparatus by  
a management apparatus, comprising the steps of, in the  
management apparatus, preparing a key file storing  
5 encrypted content key data and encrypted usage control  
policy data indicating the handling of the content data,  
in the data providing apparatus, distributing a module  
storing the content data encrypted by using the content  
key data and the key file received from the management  
10 apparatus to the data processing apparatus by using a  
predetermined communication protocol but in a format not  
depending upon the related communication protocol or  
recording the same on a storage medium, and in the data  
processing apparatus, decrypting the content key data and  
15 the usage control policy data stored in the distributed  
module and determining the handling of the content data  
based on the related decrypted usage control policy data.

Also, a data providing method of a 40th aspect of  
the present invention is a data providing method for  
20 distributing content data from a data providing apparatus  
to a data processing apparatus and managing the data  
providing apparatus and the data processing apparatus by  
a management apparatus, comprising the steps of, in the  
management apparatus, preparing a key file storing  
25 encrypted content key data and encrypted usage control

policy data indicating the handling of the content data,  
in the data providing apparatus, individually  
distributing the content data encrypted by using the  
content key data and the key file received from the  
5 management apparatus to the data processing apparatus by  
using a predetermined communication protocol but in a  
format not depending upon the related communication  
protocol or recording the same on a storage medium, and  
in the data processing apparatus, decrypting the content  
10 key data and the usage control policy data stored in the  
distributed key file and determining the handling of the  
distributed content data based on the related decrypted  
usage control policy data.

Also, a data providing method of a 41st aspect of  
15 the present invention is a data providing method for  
distributing content data from a data providing apparatus  
to a data processing apparatus and managing the data  
providing apparatus and the data processing apparatus by  
a management apparatus, comprising the steps of, in the  
20 management apparatus, preparing a key file storing  
encrypted content key data and encrypted usage control  
policy data indicating the handling of the content data  
and distributing the related produced key file to the  
data processing apparatus, in the data providing  
25 apparatus, distributing the content data encrypted by

using the content key data to the data processing  
apparatus by using a predetermined communication protocol  
but in a format not depending upon the related  
communication protocol or recording the same on a storage  
5 medium, and in the data processing apparatus, decrypting  
the content key data and the usage control policy data  
stored in the distributed key file and determining the  
handling of the distributed content data based on the  
related decrypted usage control policy data.

10 Also, a data providing method of a 42nd aspect of  
the present invention is a data providing method for  
distributing content data from a data providing apparatus  
to a data processing apparatus and managing the data  
providing apparatus and the data processing apparatus by  
15 a management apparatus, comprising the steps of, in the  
management apparatus, preparing encrypted content key  
data and encrypted usage control policy data indicating  
the handling of the content data, in the data providing  
apparatus, individually distributing the content data  
20 encrypted by using the content key data and the encrypted  
content key data and the encrypted usage control policy  
data received from the management apparatus to the data  
processing apparatus by using a predetermined  
communication protocol but in a format not depending upon  
25 the related communication protocol or recording the same



on a storage medium, and in the data processing  
apparatus, decrypting the distributed content key data  
and the usage control policy data and determining the  
handling of the content data stored in the distributed  
5 content file based on the related decrypted usage control  
policy data.

Also, a data providing method of a 43rd aspect of  
the present invention is a data providing method for  
distributing content data from a data providing apparatus  
10 to a data processing apparatus and managing the data  
providing apparatus and the data processing apparatus by  
a management apparatus, comprising the steps of, in the  
management apparatus, preparing encrypted content key  
data and encrypted usage control policy data indicating  
15 the handling of the content data and distributing the  
same to the data processing apparatus, in the data  
providing apparatus, distributing the content data  
encrypted by using the content key data to the data  
processing apparatus by using a predetermined  
20 communication protocol but in a format not depending upon  
the related communication protocol or recording the same  
on a storage medium, and in the data processing  
apparatus, decrypting the distributed content key data  
and the usage control policy data and determining the  
25 handling of the distributed content data based on the

related decrypted usage control policy data.

Also, a data providing method of a 44th aspect of the present invention is a data providing method using a data providing apparatus, a data distribution apparatus, and a data processing apparatus, comprising the steps of providing a first module storing content data encrypted by using content key data, encrypted the content key data, and encrypted usage control policy data indicating the handling of the content data from the data providing apparatus to the data distribution apparatus, distributing a second module storing the encrypted content data, content key data, and the usage control policy data stored in the provided the first module from the data distribution apparatus to the data processing apparatus by using the content key data to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and in the data processing apparatus, decrypting the content key data and the usage control policy data stored in the distributed second module and determining the handling of the content data based on the related decrypted usage control policy data.

Also, a data providing method of a 45th aspect of the present invention is a data providing method for

providing content data from a data providing apparatus to  
a data distribution apparatus, distributing the content  
data from the data distribution apparatus to a data  
processing apparatus, and managing the data providing  
5 apparatus, the data distribution apparatus, and the data  
processing apparatus by a management apparatus,  
comprising the steps of, in the management apparatus,  
preparing a key file storing encrypted content key data  
and encrypted usage control policy data indicating the  
10 handling of the content data, distributing the related  
produced key file from the management apparatus to the  
data providing apparatus, providing a first module  
storing a content file storing the content data encrypted  
by using the content key data and the key file received  
15 from the management apparatus from the data providing  
apparatus to the data distribution apparatus, and  
distributing a second module storing the provided content  
file and the key file from the data distribution  
apparatus to the data processing apparatus by using a  
20 predetermined communication protocol but in a format not  
depending upon the related communication protocol or  
recording the same on a storage medium, and in the data  
processing apparatus, decrypting the content key data and  
the usage control policy data stored in the distributed  
25 second module and determining the handling of the content

data stored in the distributed second module based on the related decrypted usage control policy data.

Also, a data providing method of a 46th aspect of the present invention is a data providing method for

5 providing content data from a data providing apparatus to a data distribution apparatus, distributing the content data from the data distribution apparatus to a data processing apparatus, and managing the data providing apparatus, the data distribution apparatus and the data

10 processing apparatus by a management apparatus, comprising the steps of, in the management apparatus, preparing a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, in the data providing

15 apparatus, providing a first module storing a content file containing the content data encrypted by using the content key data and a key file received from the management apparatus to the data distribution apparatus, in the data distribution apparatus, distributing a second

20 module storing the provided content file to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and in the data processing

25 apparatus, decrypting the content key data and the usage

control policy data stored in the distributed second module and determining the handling of the content data stored in the distributed second module based on the related decrypted usage control policy data.

5       Also, a data providing method of a 47th aspect of the present invention is a data providing method for providing content data from a data providing apparatus to a data distribution apparatus, distributing the content data from the data distribution apparatus to a data  
10   processing apparatus, and managing the data providing apparatus, the data distribution apparatus, and the data processing apparatus by a management apparatus, comprising the steps of, in the management apparatus, preparing a key file storing encrypted content key data  
15   and encrypted usage control policy data indicating the handling of the content data, distributing the produced key file from the management apparatus to the data providing apparatus, individually providing a content file storing the content data encrypted by using the  
20   content key data and the key file received from the management apparatus from the data providing apparatus to the data distribution apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same  
25   on a storage medium, and individually distributing the

distributed content file and the key file from the data  
distribution apparatus to the data distribution  
apparatus, and in the data processing apparatus,  
decrypting the content key data and the usage control  
5 policy data stored in the distributed key file and  
determining the handling of the content data stored in  
the distributed content file based on the related  
decrypted usage control policy data.

Also, a data providing method of a 48th aspect of  
10 the present invention is a data providing method for  
providing content data from a data providing apparatus to  
a data distribution apparatus and managing the data  
providing apparatus and the data processing apparatus by  
a management apparatus, comprising the steps of, in the  
15 management apparatus, preparing a key file storing  
encrypted content key data and encrypted usage control  
policy data indicating the handling of the content data,  
distributing the related produced key file from the  
management apparatus to the data processing apparatus,  
20 providing a content file storing the content data  
encrypted by using the content key data from the data  
providing apparatus to the data distribution apparatus,  
distributing the provided content file from the data  
distribution apparatus to the data processing apparatus  
25 by using a predetermined communication protocol but in a

format not depending upon the related communication  
protocol or recording the same on a storage medium, and  
in the data processing apparatus, decrypting the content  
key data and the usage control policy data stored in the  
5 distributed key file and determining the handling of the  
content data stored in the distributed content file based  
on the related decrypted usage control policy data.

Also, a data providing method of a 49th aspect of  
the present invention is a data providing method for  
10 providing content data from a data providing apparatus to  
a data distribution apparatus, distributing the content  
data from the data distribution apparatus to a data  
processing apparatus, and managing the data providing  
apparatus, the data distribution apparatus, and the data  
15 processing apparatus by a management apparatus,  
comprising the steps of, in the management apparatus,  
preparing a key file storing encrypted content key data  
and encrypted usage control policy data indicating the  
handling of the content data, in the data providing  
20 apparatus, providing a first module storing the content  
data encrypted by using the content key data and the key  
file received from the management apparatus to the data  
distribution apparatus, in the data distribution  
apparatus, distributing a second module storing the  
25 provided content data and the key file to the data

processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and in the data processing apparatus, decrypting the content key data and the usage control policy data stored in the distributed second module and determining the handling of the content data stored in the distributed second module based on the related decrypted usage control policy data.

Also, a data providing method of a 50th aspect of the present invention is a data providing method for providing content data from a data providing apparatus to a data distribution apparatus, distributing the content data from the data distribution apparatus to a data processing apparatus, and managing the data providing apparatus, the data distribution apparatus, and the data processing apparatus by a management apparatus, comprising the steps of, in the management apparatus, preparing a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data, in the data providing apparatus, individually providing the content data encrypted by using the content key data and the key file received from the management apparatus to the data distribution apparatus, in the data distribution



apparatus, individually distributing the distributed content data and the key file to the data distribution apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and in the data processing apparatus, decrypting the content key data and the usage control policy data stored in the distributed key file and determining the handling of the distributed content data based on the related decrypted usage control policy data.

Also, a data providing method of a 51st aspect of the present invention is a data providing method for distributing content data from a data providing apparatus to a data processing apparatus and managing the data providing apparatus and the data processing apparatus by a management apparatus, comprising the steps of, in the management apparatus, preparing a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of the content data and distributing the related produced key file to the data processing apparatus, in the data providing apparatus, providing the content data encrypted by using the content key data to the data distribution apparatus, in the data distribution apparatus, distributing the provided content data to the data processing apparatus,

and in the data processing apparatus, decrypting the  
content key data and the usage control policy data stored  
in the distributed key file and determining the handling  
of the distributed content data based on the related  
5 decrypted usage control policy data.

Also, a data providing method of a 52nd aspect of  
the present invention is a data providing method for  
providing content data from a data providing apparatus to  
a data distribution apparatus, distributing the content  
10 data from the data distribution apparatus to a data  
processing apparatus, and managing the data providing  
apparatus, the data distribution apparatus, and the data  
processing apparatus by a management apparatus,  
comprising the steps of, in the management apparatus,  
15 providing encrypted content key data and encrypted usage  
control policy data indicating the handling of the  
content data to the data providing apparatus, in the data  
providing apparatus, individually distributing the  
content data encrypted by using the content key data and  
20 the encrypted content key data and the encrypted usage  
control policy data received from the management  
apparatus to the data distribution apparatus, in the data  
distribution apparatus, individually distributing the  
distributed content data, the encrypted content key,  
25 data, and the encrypted usage control policy data to the

data distribution apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and in the data processing

5 apparatus, decrypting the distributed content key data and the usage control policy data and determining the handling of the distributed content data based on the related decrypted usage control policy data.

Also, a data providing method of a 53rd aspect of  
10 the present invention is a data providing method for providing content data from a data providing apparatus to a data distribution apparatus, distributing the content data from the data distribution apparatus to a data processing apparatus, and managing the data providing  
15 apparatus, the data distribution apparatus, and the data processing apparatus by a management apparatus, comprising the steps of, in the management apparatus, distributing encrypted content key data and encrypted usage control policy data indicating the handling of the  
20 content data to the data processing apparatus, in the data providing apparatus, providing the content data encrypted by using the content key data to the data distribution apparatus, the data distribution apparatus distributing the provided content data to the data  
25 processing apparatus by using a predetermined

communication protocol but in a format not depending upon  
the related communication protocol by recording the same  
on a storage medium, and in the data processing  
apparatus, decrypting the distributed content key data  
5 and the usage control policy data and determining the  
handling of the distributed content data based on the  
related decrypted usage control policy data.

Also, a data providing method of a 54th aspect of  
the present invention is a data providing method using a  
10 data providing apparatus, a data distribution apparatus,  
a management apparatus, and a data processing apparatus,  
wherein the data providing apparatus provides master  
source data of content to the management apparatus, the  
management apparatus manages the data providing  
15 apparatus, the data distribution apparatus, and the data  
processing apparatus, encrypts the provided master source  
data by using content key data to produce content data,  
produces a content file storing the related content data,  
produces a key file storing the encrypted content key  
20 data and encrypted usage control policy data indicating  
the handling of the content data, and provides the  
content file and the key file to the data distribution  
apparatus, the data distribution apparatus distributes  
the provided content file and the key file to the data  
25 processing apparatus by using a predetermined

communication protocol but in a format not depending upon  
the related communication protocol or by recording the  
same on a storage medium, and the data processing  
apparatus decrypts the content key data and the usage  
5 control policy data stored in the distributed key file  
and determines the handling of the content data stored in  
the distributed content file based on the related  
decrypted usage control policy data.

Also, a data providing method of a 55th aspect of  
10 the present invention is a data providing method using a  
data providing apparatus, a data distribution apparatus,  
a management apparatus, and a data processing apparatus,  
wherein the data providing apparatus provides master  
source data of content to the management apparatus, the  
15 management apparatus manages the data providing  
apparatus, the data distribution apparatus, and the data  
processing apparatus, encrypts the provided master source  
data by using content key data to produce content data,  
produces a content file storing the related content data,  
20 produces a key file storing the encrypted content key  
data and encrypted usage control policy data indicating  
the handling of the content data, and provides the  
content file to the data distribution apparatus and  
provides the key file to the data processing apparatus,  
25 the data distribution apparatus distributes the provided

content file to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or by recording the same on a storage medium, and the data

5 processing apparatus decrypts the content key data and the usage control policy data stored in the provided key file and determines the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

10 Also, a data providing method of a 56th aspect of the present invention is a data providing method using a data providing apparatus, a data distribution apparatus, a management apparatus, and a data processing apparatus, wherein the data providing apparatus provides a content  
15 file storing encrypted content data using content key data to the management apparatus, the management apparatus manages the data providing apparatus, the data distribution apparatus, and the data processing apparatus, produces a key file storing the encrypted  
20 content key data and encrypted usage control policy data indicating the handling of the content data, and provides the content file provided from the data providing apparatus and the produced key file to the data  
25 distributes the provided content file and the key file to

the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or by recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key file and determines the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

Also, a data providing method of a 57th aspect of the present invention is a data providing method using a data providing apparatus, a data distribution apparatus, a management apparatus, and a data processing apparatus, wherein the data providing apparatus provides a content file storing encrypted content data using content key data to the management apparatus, the management apparatus manages the data providing apparatus, the data distribution apparatus, and the data processing apparatus, produces a key file storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data, provides the content file provided from the data providing apparatus to the data distribution apparatus and provides the produced key file to the data processing apparatus, the data distribution apparatus distributes the provided

content file to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or by recording the same on a storage medium, and the data  
5 processing apparatus decrypts the content key data and the usage control policy data stored in the provided key file and determines the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

10 Also, a data providing method of a 58th aspect of the present invention is a data providing method using a data providing apparatus, a data distribution apparatus, a management apparatus, a database device, and a data processing apparatus, wherein the data providing  
15 apparatus encrypts content data by using content key data, produces a content file storing the related encrypted content data, and stores the related produced content file and a key file provided from the management apparatus in the database device, the management  
20 apparatus produces a key file storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data and provides the related produced key file to the data providing apparatus, the data distribution apparatus distributes  
25 the content file and key file obtained from the database



device to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or by recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key file and determines the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

Also, a data providing method of a 59th aspect of the present invention is a data providing method using a data providing apparatus, a data distribution apparatus, a management apparatus, a database device, and a data processing apparatus, wherein the data providing apparatus encrypts content data by using content key data, produces a content file storing the related encrypted content data, and stores the related produced content file in the database device, the management apparatus produces a key file storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data and provides the related produced key file to the data distribution apparatus, the data distribution apparatus distributes the content file obtained from the database device and the key file provided from the data distribution

apparatus to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or by recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key file and determines the handling of the content data stored in the distributed content file based on the related decrypted usage control policy data.

Also, a data providing method of a 60th aspect of the present invention is a data providing method using a data providing apparatus, a data distribution apparatus, a management apparatus, a database device, and a data processing apparatus, wherein the data providing apparatus encrypts content data by using content key data, produces a content file storing the related encrypted content data, and stores the related produced content file in the database device, the management apparatus produces a key file storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data and provides the related produced key file to the data processing apparatus, the data distribution apparatus distributes the content file obtained from the database device to the data processing apparatus by using a predetermined

communication protocol but in a format not depending upon  
the related communication protocol or by recording the  
same on a storage medium, and the data processing  
apparatus decrypts the content key data and the usage  
5 control policy data stored in the provided key file and  
determines the handling of the content data stored in the  
distributed content file based on the related decrypted  
usage control policy data.

Also, a data providing method of a 61st aspect of  
10 the present invention is a data providing method using a  
plurality of data providing apparatuses, a data  
distribution apparatus, a plurality of management  
apparatuses, a database device, and a data processing  
apparatus, wherein the data providing apparatuses encrypt  
15 content data by using content key data, produce content  
files storing the related encrypted content data, and  
store the related produced content files and key files  
provided from corresponding management apparatuses in the  
database device, the management apparatuses produce key  
20 files storing the encrypted content key data and  
encrypted usage control policy data indicating the  
handling of the content data for the content data  
provided by corresponding data providing apparatuses and  
provide the related produced key files to corresponding  
25 data providing apparatuses, the data distribution

apparatus distributes the content files and key files  
obtained from the database device to the data processing  
apparatus by using a predetermined communication protocol  
but in a format not depending upon the related  
5 communication protocol or by recording the same on a  
storage medium, and the data processing apparatus  
decrypts the content key data and the usage control  
policy data stored in the distributed key files and  
determines the handling of the content data stored in the  
10 distributed content files based on the related decrypted  
usage control policy data.

Also, a data providing method of a 62nd aspect of  
the present invention is a data providing method using a  
plurality of data providing apparatuses, a data  
15 distribution apparatus, a plurality of management  
apparatuses, a database device, and a data processing  
apparatus, wherein the data providing apparatuses encrypt  
content data by using content key data, produce content  
files storing the related encrypted content data, and  
20 store the related produced content files in the database  
device, the management apparatuses produce key files  
storing the encrypted content key data and encrypted  
usage control policy data indicating the handling of the  
content data for the content data provided by  
25 corresponding data providing apparatuses and provide the

related produced key files to the data distribution  
apparatus, the data distribution apparatus distributes  
the content files obtained from the database device and  
the key files provided from the management apparatuses to  
5 the data processing apparatus by using a predetermined  
communication protocol but in a format not depending upon  
the related communication protocol or by recording the  
same on a storage medium, and the data processing  
apparatus decrypts the content key data and the usage  
10 control policy data stored in the distributed key files  
and determines the handling of the content data stored in  
the distributed content files based on the related  
decrypted usage control policy data.

Also, a data providing method of a 63rd aspect of  
15 the present invention is a data providing method using a  
plurality of data providing apparatuses, a data  
distribution apparatus, a plurality of management  
apparatuses, a database device, and a data processing  
apparatus, wherein the data providing apparatuses encrypt  
20 content data by using content key data, produce content  
files storing the related encrypted content data, and  
store the related produced content files in the database  
device, the management apparatuses produce key files  
storing the encrypted content key data and encrypted  
25 usage control policy data indicating the handling of the

content data for the content data provided by  
corresponding data providing apparatuses and provide the  
related produced key files to the data processing  
apparatus, the data distribution apparatus distributes  
5 the content files obtained from the database device to  
the data processing apparatus by using a predetermined  
communication protocol but in a format not depending upon  
the related communication protocol or by recording the  
same on a storage medium, and the data processing  
10 apparatus decrypts the content key data and the usage  
control policy data stored in the provided key files and  
determines the handling of the content data stored in the  
distributed content files based on the related decrypted  
usage control policy data.

15 Also, a data providing method of a 64th aspect of  
the present invention is a data providing method using a  
plurality of data providing apparatuses, a data  
distribution apparatus, a plurality of management  
apparatuses, a database device, and a data processing  
20 apparatus, wherein the data providing apparatuses provide  
master sources of content data to corresponding  
management apparatuses and store content files and key  
files received from the related management apparatuses in  
the database, the management apparatuses encrypt the  
25 master sources received from corresponding data providing

apparatuses by using content key data, produce content files storing the related encrypted content data, produce key files storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data for the content data provided by corresponding data providing apparatuses, and send the produced content files and the produced key files to corresponding data providing apparatuses, the data distribution apparatus distributes the content files and key files obtained from the database device to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or by recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key files and determines the handling of the content data stored in the distributed content files based on the related decrypted usage control policy data.

Also, a data providing method of a 65th aspect of the present invention is a data providing method using a plurality of data providing apparatuses, a data distribution apparatus, a plurality of management apparatuses, a database device, and a data processing apparatus, wherein the data providing apparatuses provide

master sources of content data to corresponding management apparatuses and store content files received from the related management apparatuses in the database, the management apparatuses encrypt the master sources

5 received from corresponding data providing apparatuses by using content key data, produce content files storing the related encrypted content data, send the related produced content files to the data providing apparatuses, produce key files storing the encrypted content key data and

10 encrypted usage control policy data indicating the handling of the content data for the content data provided by corresponding data providing apparatuses, send the related produced key files to corresponding data distribution apparatus, the data distribution apparatus

15 distributes the content files obtained from the database device and the key files provided from the management apparatuses to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or by

20 recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed key files and determines the handling of the content data stored in the distributed content files based on the

25 related decrypted usage control policy data.



Also, a data providing method of a 66th aspect of the present invention is a data providing method using a plurality of data providing apparatuses, a data distribution apparatus, a plurality of management apparatuses, a database device, and a data processing apparatus, wherein the data providing apparatuses provide master sources of content data to corresponding management apparatuses and store content files received from the related management apparatuses in the database, the management apparatuses encrypt the master sources received from corresponding data providing apparatuses by using content key data, produce content files storing the related encrypted content data, send the related produced content files to the data providing apparatuses, produce key files storing the encrypted content key data and encrypted usage control policy data indicating the handling of the content data for the content data provided by corresponding data providing apparatuses, and provide the related produced key files to the data processing apparatus, the data distribution apparatus distributes the content files obtained from the database device to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or by recording the same on a storage medium, and the data

processing apparatus decrypts the content key data and the usage control policy data stored in the provided key files and determines the handling of the content data stored in the distributed content files based on the related decrypted usage control policy data.

Also, a data providing method of a 67th aspect of the present invention is a data providing method using a data providing apparatus, a data distribution apparatus, and a data processing apparatus, wherein the data providing apparatus provides a first module storing content data encrypted by using content key data, the encrypted content key data, and encrypted usage control policy data indicating the handling of the content data to the data distribution apparatus, performs charge processing in units of the content data based on log data received from the data processing apparatus, performs profit distribution processing for distributing the profit paid by interested parties of the data processing apparatus to interested parties of the related data providing apparatus and interested parties of the data distribution apparatus, the data distribution apparatus distributes a second module storing the encrypted content data, content key data and usage control policy data stored in the provided first module to the data processing apparatus by using a predetermined

communication protocol but in a format not depending upon  
the related communication protocol or by recording the  
same on a storage medium, and the data processing  
apparatus decrypts the content key data and the usage  
5 control policy data stored in the distributed module,  
determines the handling of the content data based on the  
related decrypted usage control policy data, produces the  
log data for the handling of the related content data and  
sends the related log data to the data providing  
10 apparatus.

Also, a data providing method of a 68th aspect of  
the present invention is a data providing method using a  
data providing apparatus, a data distribution apparatus,  
a data processing apparatus, and a management apparatus,  
15 wherein the data providing apparatus provides content  
data, the data distribution apparatus distributes the  
content file provided from the data providing apparatus  
or a content file in accordance with the content data  
provided by the data providing apparatus received from  
20 the management apparatus to the data processing  
apparatus, and the data processing apparatus decrypts the  
usage control policy data stored in the key file received  
from the data distribution apparatus or the management  
apparatus, determines the handling of the content data  
25 stored in the content file received from the data

distribution apparatus or the management apparatus based  
on the related decrypted usage control policy data, and  
further distributes the content file and key file  
received from the data distribution apparatus or the  
5 management apparatus to the other data processing  
apparatus.

Also, a data providing system of a 71st aspect of  
the present invention is a data providing system for  
distributing content data from a data providing apparatus  
10 to a data processing apparatus, wherein the data  
providing apparatus distributes a module storing content  
data encrypted by using content key data, the encrypted  
content key data, and encrypted usage control policy data  
indicating the handling of the content data in a format  
15 not depending upon at least one among existence of a  
compression of the content data, a compression method, a  
method of the encryption, and parameters of a signal  
giving the content data to the data processing apparatus  
by using a predetermined communication protocol but in a  
20 format not depending upon the related communication  
protocol or by recording the same on a storage medium,  
and the data processing apparatus decrypts the content  
key data and the usage control policy data stored in the  
distributed module and determines the handling of the  
25 content data based on the related decrypted usage control

policy data.

Also, a data providing system of a 72nd aspect of the present invention is a data providing system having a data providing apparatus, a data distribution apparatus, and a data processing apparatus, wherein the data providing apparatus distributes a first module storing content data encrypted by using content key data, the encrypted content key data, and encrypted usage control policy data indicating the handling of the content data in a format not depending upon at least one among existence of compression of the content data, a compression method, a method of the encryption, and parameters of a signal giving the content data to the data distribution apparatus, the data distribution apparatus distributes a second module storing the encrypted content data, content key data, and the usage control policy data stored in the provided first module to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or by recording the same on a storage medium, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed second module and determines the handling of the content data based on the related decrypted usage control policy data.

Also, a data providing system of a 73rd aspect of the present invention is a data providing system having a data providing apparatus, a data distribution apparatus, and a data processing apparatus, wherein the data providing apparatus distributes a first module storing content data encrypted by using content key data, the encrypted content key data, and encrypted usage control policy data indicating the handling of the content data to the data distribution apparatus, the data distribution apparatus encrypts a plurality of second modules storing the encrypted content data, content key data, and the usage control policy data stored in the provided first module by using a common key obtained by mutual certification with the data processing apparatus, and then distributes the same to the data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol, and the data processing apparatus has a first processing circuit for decrypting the distributed plurality of second modules by using the common key, selecting a single or a plurality of second modules from among the related decrypted plurality of second modules, and performing charge processing with respect to a distribution service of the second modules and a tamper resistant second processing circuit

receiving the selected the second modules, decrypting the content key data and the usage control policy data stored in the related second modules, and determining the handling of the content data based on the related  
5 decrypted usage control policy data.

#### BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a view of the overall configuration of an EMD system of a first embodiment of the present invention,

10 Fig. 2 is a view for explaining a concept of a secure container of the present invention,

Fig. 3 is a functional block diagram of a content provider shown in Fig. 1 and a view of a flow of data related to data transmitted and received with a SAM of a  
15 user home network,

Fig. 4 is a functional block diagram of the content provider shown in Fig. 1 and a view of the flow of data related to the data transmitted and received between the content provider and an EMD service center,

20 Figs. 5A to 5C are views for explaining a format of the secure container transmitted from the content provider shown in Fig. 1 to the SAM,

Fig. 6 is a view for explaining data contained in a content file shown in Fig. 5 in detail,

25 Fig. 7 is a view for explaining data contained in a

key file shown in Fig. 5 in detail,

Fig. 8 is a view for explaining a header data stored  
in the content file,

Fig. 9 is a view for explaining a content ID,

5 Fig. 10 is a view for explaining a directory  
structure of the secure container,

Fig. 11 is a view for explaining a hyper link  
structure of the secure container,

10 Fig. 12 is a view for explaining a first example of  
ROM type storage medium used in the present embodiment,

Fig. 13 is a view for explaining a second example of  
the ROM type storage medium used in the present  
embodiment,

15 Fig. 14 is a view for explaining a third example of  
the ROM type storage medium used in the present  
embodiment,

Fig. 15 is a view for explaining a first example of  
RAM type storage medium used in the present embodiment,

20 Fig. 16 is a view for explaining a second example of  
the RAM type storage medium used in the present  
embodiment,

Fig. 17 is a view for explaining a third example of  
the RAM type storage medium used in the present  
embodiment,

25 Fig. 18 is a view for explaining a registration



request use module transmitted from the content provider to the EMD service center,

Fig. 19 is a flowchart showing a routine of processing for registration from the content provider to  
5 the EMD service center,

Fig. 20 is a flowchart showing a routine of processing for preparation of an explanation in the content provider,

Fig. 21 is a flowchart showing a routine of  
10 processing for preparation of an explanation in the content provider,

Fig. 22 is a flowchart showing a routine of processing for preparation of an explanation in the content provider,

15 Fig. 23 is a functional block diagram of the EMD service center shown in Fig. 1 and a view of the flow of the data related to the data transmitted and received with the content provider,

Fig. 24 is a functional block diagram of the EMD  
20 service center shown in Fig. 1 and a view of the flow of the data related to the data transmitted and received between the SAM and a settlement manager shown in Fig. 1,

Fig. 25 is a view of the configuration of network apparatuses in the user home network shown in Fig. 1,

25 Fig. 26 is a functional block diagram of a SAM in

the user home network shown in Fig. 1 and a view of the flow of the data until the secure container received from the content provider is decrypted,

Fig. 27 is a view for explaining data stored in an  
5 external memory shown in Fig. 25,

Fig. 28 is a view for explaining data stored in a stack memory,

Fig. 29 is another view of the configuration of the network apparatus in the user home network shown in Fig.  
10 1,

Fig. 30 is a view for explaining data stored in a storage unit shown in Fig. 26,

Fig. 31 is a functional block diagram of the SAM in the user home network shown in Fig. 1 and a view of the  
15 flow of the data related to processing for using and/or purchasing the content data,

Fig. 32 is a view for explaining the flow of processing in a transferring side SAM in a case where the content file which is downloaded on a download memory of  
20 the network apparatus shown in Fig. 25 and with a purchase form already determined therefor is transferred to the SAM of an AV apparatus,

Fig. 33 is a view of the flow of the data in the transferring side SAM in the case shown in Fig. 32,

25 Figs. 34A to 34D are views for explaining the format

of the secure container for which the purchase form is determined,

Fig. 35 is a view of the flow of the data when writing the input content file etc. in a RAM type or ROM type storage medium in the transferring side SAM in the case shown in Fig. 32,

Fig. 36 is a view for explaining the flow of processing when determining the purchase form in an AV apparatus in a case where the user home network is receives the ROM type storage medium shown in Fig. 7 for which the purchase form of the content has not been determined off-line,

Fig. 37 is a view of the flow of the data in the SAM in the case shown in Fig. 36,

Fig. 38 is a view for explaining the flow of processing when reading the secure container from the ROM type storage medium with the purchase form not yet determined in the AV apparatus in the user home network, transferring this to another AV apparatus, and writing the same in a RAM type storage medium,

Fig. 39 is a view of the flow of the data in the transferring side SAM in the case shown in Fig. 38,

Figs. 40A to 40C are views for explaining the format of the secure container transferred from the transferring side SAM to a transferred side SAM in Fig. 38,

Fig. 41 is a view of the flow of data in the transferred side SAM in the case shown in Fig. 38,

Figs. 42A to 42F are views for explaining the format of the data transmitted and received among the content provider shown in Fig. 1, EMD service center, and SAM by an In-band method, and an out-of-band method,

Figs. 43G to 43J are views for explaining the format of the data transmitted and received among the content provider shown in Fig. 1, EMD service center, and SAM by the in-band method and the out-of-band method,

Fig. 44 is a view for explaining an example of a connection configuration of apparatuses to buses in the user home network,

Fig. 45 is a view for explaining the data format of a SAM registration list produced by a SAM,

Fig. 46 is a view for explaining the data format of the SAM registration list produced by the EMD service center,

Fig. 47 is a flowchart of the overall operation of the content provider shown in Fig. 1,

Fig. 48 is a view for explaining an example of a delivery protocol of the secure container used in the EMD system of a first embodiment,

Fig. 49 is a view for explaining a second modification of the first embodiment of the present

invention,

Fig. 50 is a view for explaining a third modification of the first embodiment of the present invention,

5 Fig. 51 is a view for explaining a case where a first procedure is employed in a fourth modification of the first embodiment of the present invention,

Fig. 52 is a view for explaining a case where a second procedure is employed in a fourth modification of the first embodiment of the present invention,

Fig. 53 is a view for explaining a fifth modification of the first embodiment of the present invention,

Fig. 54 is a view for explaining a first pattern of a sixth modification of the first embodiment of the present invention,

Fig. 55 is a view for explaining a second pattern of a sixth modification of the first embodiment of the present invention,

20 Fig. 56 is a view for explaining a third pattern of a sixth modification of the first embodiment of the present invention,

Fig. 57 is a view for explaining a fourth pattern of a sixth modification of the first embodiment of the present invention,

25

Fig. 58 is a view for explaining a fifth pattern of a sixth modification of the first embodiment of the present invention,

Fig. 59 is an overall view of the configuration of the EMD system of a second embodiment of the present invention,

Fig. 60 is a functional block diagram of the content provider shown in Fig. 59 and a view of the flow of the data related to the secure container transmitted to a service provider,

Fig. 61 is a flowchart showing a routine of processing for delivery of the secure container performed in the content provider,

Fig. 62 is a flowchart showing a routine of the processing for delivery of the secure container performed in the content provider,

Fig. 63 is a functional block diagram of the service provider shown in Fig. 59 and a view of the flow of the data transmitted and received with the user home network,

Fig. 64 is a flowchart showing a routine of the processing for preparation of the secure container performed in the service provider,

Figs. 65A to 65D are views for explaining the format of the secure container transmitted from the service provider shown in Fig. 59 to the user home network,

Fig. 66 is a view for explaining a transmission  
format of the content file stored in the secure container  
shown in Fig. 65,

Fig. 67 is a view for explaining the transmission  
format of the key file stored in the secure container  
shown in Fig. 65,

Fig. 68 is a functional block diagram of the service  
provider shown in Fig. 59 and a view of the flow of the  
data transmitted and received with the EMD service  
center,

Fig. 69 is a view for explaining the format of a  
price tag registration request use module transmitted  
from the service provider to the EMD service center,

Fig. 70 is a functional block diagram of the EMD  
service center shown in Fig. 59 and a view of the flow of  
the data related to the data transmitted and received  
with the service provider,

Fig. 71 is a functional block diagram of the EMD  
service center shown in Fig. 59 and a view of the flow of  
the data related to the data transmitted and received  
with the content provider,

Fig. 72 is a functional block diagram of the EMD  
service center shown in Fig. 59 and a view of the flow of  
the data related to the data transmitted and received  
with the SAM,

Fig. 73 is a view for explaining contents of usage log data,

Fig. 74 is a view of the configuration of the network apparatus shown in Fig. 59,

5 Fig. 75 is a functional block diagram of a CA module shown in Fig. 74,

Fig. 76 is a functional block diagram of the SAM shown in Fig. 74 and a view of the flow of the data from the input of the secure container to decryption,

10 Fig. 77 is a view for explaining the data stored in the storage unit shown in Fig. 76,

Fig. 78 is a functional block diagram of the SAM shown in Fig. 74 and a view of the flow of the data in a case where a purchase and/or usage form of the content  
15 etc. are determined,

Fig. 79 is a flowchart showing a routine of processing for determining the purchase form of the secure container in the SAM,

Fig. 80 is a view for explaining the format of the  
20 key file after the purchase form is determined,

Figs. 81A to 81E are views for explaining the flow of the processing in the transferred side SAM in a case where the content file downloaded on the download memory of the network apparatus shown in Fig. 74 and with the  
25 purchase form already determined therefor is transferred



to the SAM of the AV apparatus,

Fig. 82 is a view of the flow of the data in the transferring side SAM in the case shown in Fig. 81,

Fig. 83 is a view of the flow of the data in the transferred side SAM in the case shown in Fig. 81,

Fig. 84 is a flowchart of the overall operation of the EMD system shown in Fig. 59,

Fig. 85 is a flowchart of the overall operation of the EMD system shown in Fig. 59,

Fig. 86 is a view for explaining an example of the delivery format of the secure container from the service provider to the user home network in the EMD system of the second embodiment,

Fig. 87 is a view for explaining an example of the delivery protocol of the secure container employed by the EMD system of the second embodiment,

Fig. 88 is a view for explaining the delivery protocol used when delivering the secure container etc. from the user home network to a service provider 310 in Fig. 87,

Fig. 89 is a view for explaining the delivery protocol used when delivering the key file etc. from the content provider to the EMD service center in Fig. 87,

Fig. 90 is a view for explaining the delivery protocol used when delivering a price tag data 312 etc.

from the service provider to the EMD service center in  
Fig. 87,

Fig. 91 is a view for explaining the delivery  
protocol used when delivering the secure container etc.

5 in the user home network in Fig. 87,

Fig. 92 is a view for explaining an implement format  
of the secure container to a protocol layer in a case  
where XML/SMIL/BML is utilized for a data broadcast  
method of a digital broadcast,

10 Fig. 93 is a view for explaining the implement  
format of the secure container to the protocol layer in a  
case where MHEG is utilized for the data broadcast method  
of the digital broadcast,

Fig. 94 is a view for explaining the implement  
15 format of the secure container to the protocol layer in a  
case where XML/SMIL is utilized for the data broadcast  
method of an interface,

Fig. 95 is a view for explaining the delivery  
protocol used when delivering the usage log data etc.  
20 from the user home network to the EMD service center,

Fig. 96 is a view for explaining the delivery  
protocol used when delivering the secure container etc.  
in the user home network,

Fig. 97 is a view of the configuration of the EMD  
25 system using two service providers according to a first

modification of the second embodiment of the present invention,

Fig. 98 is a view of the configuration of the EMD system using a plurality of content providers according to a second modification of the second embodiment of the present invention,

Fig. 99 is a view of the configuration of the EMD system according to a third modification of the second embodiment of the present invention,

Fig. 100 is a view of the configuration of the EMD system according to a fourth modification of the second embodiment of the present invention,

Fig. 101 is a view for explaining a form of a route for acquiring certificate data,

Fig. 102 is a view for explaining processing in a case where the certificate data of the content provider is invalidated,

Fig. 103 is a view for explaining processing in a case where the certificate data of the service provider is invalidated,

Fig. 104 is a view for explaining processing in a case where the certificate data of the SAM is invalidated,

Fig. 105 is a view for explaining another processing in the case where the certificate data of the SAM is

invalidated,

Fig. 106 is a view for explaining a case where a right management use clearinghouse and an electronic settlement use clearinghouse are provided in the EMD system shown in Fig. 47 in place of the EMD service center,

Fig. 107 is a view of the configuration of the EMD system in a case where the right management use clearinghouse and the electronic settlement use clearinghouse shown in Fig. 106 are provided in a single EMD service center,

Fig. 108 is a view of the configuration of the EMD system in a case where the service provider directly performs settlement at the electronic settlement use clearinghouse,

Fig. 109 is a view of the configuration of the EMD system in a case where the content provider directly performs settlement at the electronic settlement use clearinghouse,

Fig. 110 is a view of the configuration of the EMD system in a case where the content provider is further provided with functions of both of the right management use clearinghouse and the electronic settlement use clearinghouse,

Fig. 111 is a view for explaining the format of the

secure container provided from the content provider to the service provider shown in Fig. 47 in an eighth modification of the second embodiment of the present invention,

5        Fig. 112 is a view for explaining a link relationship by directory structure data between the content file and the key file shown in Fig. 111,

         Fig. 113 is a view for explaining another example of the directory structure between the content file and the  
10    key file,

         Fig. 114 is a view for explaining the format of the secure container provided from the service provider to the SAM shown in Fig. 47 in the eighth modification of the second embodiment of the present invention,

15        Fig. 115 is a view for explaining a first concept of the data format of a composite type secure container,

         Fig. 116 is a view for explaining a second concept of the data format of the composite type secure container,

20        Fig. 117 is a view for explaining a case where a first procedure is employed in the EMD system according to the eighth modification of the second embodiment of the present invention,

         Fig. 118 is a view for explaining a case where a  
25    second procedure is employed in the EMD system according

to the eighth modification of the second embodiment of the present invention,

Fig. 119 is a view for explaining a data format in a case where the file format is not employed in the EMD system according to the eighth modification of the second embodiment of the present invention,

Fig. 120 is a view of the configuration of the EMD system according to a 10th modification of the second embodiment of the present invention,

Fig. 121 is a view of the configuration of the EMD system according to a first pattern of an 11th modification of the second embodiment of the present invention,

Fig. 122 is a view of the configuration of the EMD system according to a second pattern of the 11th modification of the second embodiment of the present invention,

Fig. 123 is a view of the configuration of the EMD system according to a third pattern of the 11th modification of the second embodiment of the present invention,

Fig. 124 is a view of the configuration of the EMD system according to a fourth pattern of the 11th modification of the second embodiment of the present invention,

Fig. 125 is a view of the configuration of the EMD system according to a fifth pattern of the 11th modification of the second embodiment of the present invention,

5        Fig. 126 is a view of the configuration of the EMD system according to a ninth modification of the second embodiment of the present invention,

Fig. 127 is a view for explaining a file inclusion size relationship of the secure container in the second  
10        embodiment of the present invention,

Fig. 128 is a view for explaining the EMD system of a third embodiment of the present invention,

Fig. 129 is a functional block diagram of the EMD service center shown in Fig. 128,

15        Fig. 130 is a view for explaining a modification of the EMD system of the third embodiment of the present invention,

Fig. 131 is a view for explaining the EMD system of a fourth embodiment of the present invention,

20        Fig. 132 is a view for explaining a modification of the EMD system of the fourth embodiment of the present invention,

Fig. 133 is a view for explaining the EMD system of a fifth embodiment of the present invention,

25        Fig. 134 is a view for explaining a modification of

the EMD system of the fifth embodiment of the present invention,

Fig. 135 is a view for explaining another modification of the EMD system of the fifth embodiment of the present invention,

Fig. 136 is a view for explaining the EMD system of a sixth embodiment of the present invention,

Fig. 137 is a view for explaining a modification of the EMD system of the sixth embodiment of the present invention,

Fig. 138 is a view for explaining another modification of the EMD system of the sixth embodiment of the present invention,

Fig. 139 is a view for explaining the EMD system of a seventh embodiment of the present invention,

Fig. 140 is a view for explaining a modification of the EMD system of the seventh embodiment of the present invention,

Fig. 141 is a view for explaining another modification of the EMD system of the seventh embodiment of the present invention,

Fig. 142 is a view for explaining the EMD system of an eighth embodiment of the present invention,

Fig. 143 is a view for explaining the EMD system of a ninth embodiment of the present invention,



Fig. 144 is a view for explaining the format of the key file in a case where the key file is produced in the content provider, and

Fig. 145 is a view of the configuration of a  
5 conventional EMD system.

#### BEST MODE FOR WORKING THE INVENTION

Below, an explanation will be given of an EMD (electronic music distribution) system according to the present embodiment.

#### 10 First embodiment

Figure 1 is a view of the configuration of an EMD system 100 of the present embodiment.

In the present embodiment, the content data distributed to the user means digital data with the  
15 information per se having value and includes image data, audio data, programs (software), etc., but an explanation will be given below by taking as an example music data.

As shown in Fig. 1, the EMD system 100 has a content provider 101, an EMD service center (clearinghouse,  
20 hereinafter, also described as an "ESC") 102, and a user home network 103.

Here, the content provider 101, EMD service center 102, and SAMs 105<sub>1</sub> to 105<sub>4</sub> correspond to the data providing apparatus, management device, and the data  
25 processing apparatuses according to claim 1, claim 6,

claim 104, and claim 109.

First, a brief explanation will be given of the EMD system 100.

In the EMD system 100, the content provider 101  
5 sends the content key data  $K_c$  used when encrypting the  
content data  $C$  of the content to be provided by itself,  
usage control policy (UCP, certificate of title) data 106  
indicating the content of rights such as usage permission  
conditions of the content data  $C$ , and electronic  
10 watermark information management data indicating the  
content and buried location of the electronic watermark  
information to the EMD service center 102 serving as the  
reputable authority manager.

The EMD service center 102 registers (certifies or  
15 authorizes) the content key data  $K_c$ , usage control policy  
data 106, and the electronic watermark information key  
data received from the content provider 101.

Also, the EMD service center 102 produces a key file  
KF with the content key data  $K_c$  encrypted by the  
20 distribution use key data  $KD_1$  to  $KD_6$  of a corresponding  
period, the usage control policy data 106, and its own  
signature data stored therein and sends this to the  
content provider 101.

Here, the signature data is used for verifying  
25 existence of tampering with the key file KF, the

legitimacy of the author of the key file KF, and the fact that the key file KF was normally registered in the EMD service center 102.

Also, the content provider 101 encrypts the content data C by the content key data Kc and distributes a secure container (module of the present invention) 104 storing the related produced content file CF, key file KF received from the EMD service center 102, its own signature data, etc. therein to the user home network 103 by using a network such as the Internet, digital broadcast, or package media such as storage media.

Here, the signature data stored in the secure container 104 is used for verifying the existence of tampering with the corresponding data and the legitimacy of the author and transmitter of the related data.

The user home network 103 has for example a network apparatus 160<sub>1</sub> and AV apparatuses 160<sub>2</sub> to 160<sub>4</sub>.

The network apparatus 160<sub>1</sub> includes a built-in SAM (secure application module) 105<sub>1</sub>.

The AV apparatuses 160<sub>2</sub> to 160<sub>4</sub> include built-in SAMs 105<sub>1</sub> to 105<sub>4</sub>. The SAMs 105<sub>1</sub> to 105<sub>4</sub> are connected to each other via a bus 191 for example an IEEE (Institute of Electrical and Electronics Engineers) 1394 serial interface bus.

The SAMs 105<sub>1</sub> to 105<sub>4</sub> decrypt the secure container

104 received by the network apparatus 160<sub>1</sub> via the network or the like from the content provider 101 on-line and/or the secure container 104 received at the AV apparatuses 160<sub>2</sub> to 160<sub>4</sub> from the content provider 101  
5 via storage media off-line by using the distribution use key data KD<sub>1</sub> to KD<sub>3</sub> of the corresponding period, then perform the verification of the signature data.

The secure container 104 supplied to the SAMs 105<sub>1</sub> to 105<sub>4</sub> becomes the object of the reproduction, recording  
10 to a storage medium etc. after the purchase and/or usage form is determined by an operation of the users in the network apparatus 160<sub>1</sub> and the AV apparatuses 160<sub>2</sub> to 160<sub>4</sub>.

The SAMs 105<sub>1</sub> to 105<sub>4</sub> record the log of the purchase  
15 and/or usage form of the secure container 104 as usage log data 108 and, at the same time, produce usage control status data 166 indicating the purchase form.

The usage log data 108 is transmitted from the user home network 103 to the EMD service center 102 in  
20 response to for example a request from the EMD service center 102.

The usage control status data 166 is transmitted from the user home network 103 to the EMD service center 102 whenever for example the purchase form is determined.

25 The EMD service center 102 determines (calculates) a

charge content based on the usage log data 108 and performs settlement at a settlement manager 91 such as a bank via a payment gateway 90. By this, the money paid to the settlement manager 91 by the user of the user home network 103 is paid to the content provider 101 by the settlement processing by the EMD service center 102.

Also, the EMD service center 102 transmits the settlement report data 107 to the content provider 101 at every predetermined period.

10 In the present embodiment, the EMD service center 102 has a certificate authority function, a key data management function, and a right clearing (profit distribution) function.

Namely, the EMD service center 102 functions as a second certificate authority with respect to a route certificate authority 92 as the highest authority manager located at a neutral position (located in the lower layer of the route certificate authority 92) and certifies the legitimacy of the related public key data by attaching a signature by secret key data of the EMD service center 102 to the certificate data of the public key data used for the verification processing of the signature data in the content provider 101 and SAMs 105<sub>1</sub> to 105<sub>4</sub>. Also, as mentioned above, the registration and authorization of the usage control policy data 106 of the content provider

101 by the EMD service center 102 is one of the certificate authority functions of the EMD service center 102.

Also, the EMD service center 102 has a key data management function for managing the key data, for example, the distribution use key data  $KD_1$  to  $KD_6$ .

Also, the EMD service center 102 has a right clearing (profit distribution) function of performing settlement for a purchase and/or usage of the content by the user based on the suggested retailer' price SRP described in the authorized usage control policy data 106 and the usage log data 108 input from the SAMs 105<sub>1</sub> to 105<sub>4</sub> and distributing money paid by the user to the content provider 101.

Figure 2 is a view summarizing the concept of the secure container 104.

As shown in Fig. 2, in the secure container 104, the content file CF produced by the content provider 101 and the key file KF produced by the EMD service center 102 are stored.

In the content file CF, header data containing the header portion and the content ID, the encrypted content data C using the content key data  $K_c$ , and the signature data using a secret key data  $K_{CP,S}$  of the content provider 101 for them are stored.

In the key file KF, the header data containing the header portion and the content ID, the content key data Kc, and the usage control policy data 106 encrypted by the distribution use key data  $KD_1$  to  $KD_6$  and the  
5 signature data by secret key data  $K_{ESC,S}$  of the EMD service center 102 for them are stored.

Below, a detailed explanation will be given of the components of the content provider 101.

[Content Provider 101]

10 Figure 3 is a functional block diagram of the content provider 101 and shows the flow of the data related to the data transmitted and received with the SAMs  $105_1$  to  $105_4$  of the user home network 103.

Also, in Fig. 4, the flow of the data related to the  
15 data transmitted and received between the content provider 101 and the EMD service center 102 is shown.

Note that, in Fig. 4 and the following drawings, the flow of the data input and output to and from the signature data processing unit and the encryption and/or  
20 decryption unit using session key data  $K_{SES}$  is omitted.

As shown in Fig. 3 and Fig. 4, the content provider 101 has a content master source database 111, an electronic watermark information addition unit 112, a compression unit 113, an encryption unit 114, a random  
25 number generation unit 115, an expansion unit 116, a

signature processing unit 117, a secure container  
preparation unit 118, a secure container database 118a, a  
key file database 118b, a storage unit (database) 119, a  
mutual certification unit 120, an encryption and/or  
5 decryption unit 121, a usage control policy data  
preparation unit 122, an audial check unit 123, a SAM  
management unit 124, an EMD service center management  
unit 125, and a content ID generation unit 850.

The content provider 101 registers for example its  
10 own generated public key data, ID, and its own bank  
account number (account number for settlement) in the EMD  
service center 102 off-line before communicating with the  
EMD service center 102 and acquires its own identifier  
(identification number) CP\_ID. Also, the content provider  
15 101 receives the public key data of the EMD service  
center 102 and the public key data of the route  
certificate authority 92 from the EMD service center 102.

Below, an explanation will be given of the  
functional blocks of the content provider 101 shown in  
20 Fig. 3 and Fig. 4.

The content master source database 111 stores the  
content data as the master source of the content to be  
provided to the user home network 103 and outputs content  
data S111 to be provided to the electronic watermark  
25 information addition unit 112.



The electronic watermark information addition unit 112 buries a source watermark Ws, a copy control watermark Wc, a user watermark Wu, a link watermark WL, etc. in the content data S111 to produce content data S112 and outputs the content data S112 to the compression unit 113.

The source watermark Ws is information concerning the copyright such as the name of the copyright owner of the content data, the ISRC code, authoring date, authoring apparatus ID (identification data), and destination of distribution of the content.

The copy control watermark Wc is information containing a copy prohibition bit for prevention of copying via an analog interface.

The user watermark Wu contains, for example, the identifier CP\_ID of the content provider 101 for specifying the origin of distribution and the destination of distribution of the secure container 104 and identifiers SAM\_ID<sub>1</sub> to SAM\_ID<sub>4</sub> of the SAMs 105<sub>1</sub> to 105<sub>4</sub> of the user home network 103.

The link watermark WL contains for example the content ID of the content data C.

By burying the link watermark WL in the content data C, even in a case where the content data C is distributed by an analog broadcast for example a television or AM/FM

radio, the EMD service center 102 can introduce a content provider 101 handling the related content data C to the user in response to a request from the user. Namely, by detecting the link watermark WL buried in the content data C utilizing an electronic watermark information decoder at the receiving location of the related content data C and transmitting the content ID contained in the related detected link watermark WL to the EMD service center 102, the EMD service center 102 can introduce the content provider 101 etc. handling the related content data C to the related user.

Concretely, for example, if the user pushes a predetermined button at a point of time when he thinks that the music being broadcast is good while listening to the radio in a car, the electronic watermark information decoder built-in the related radio detects the content ID contained in the link watermark WL buried in the related content data C, a communication address, etc. of the EMD service center 102 registering the related content data C etc., and stores the related detected data in a media SAM carried in for example a memory stick or other semiconductor memory or an MD (Mini Disc) or other optical disc or other portable medium. Then, he sets the related movable media in the network apparatus carrying a SAM connected to the network. Then, after mutual

certification by the related SAM and the EMD service center 102, he transmits the personal information carried in the media SAM and the stored content ID etc. from the network apparatus to the EMD service center 102.

5    Thereafter, the network apparatus receives an introduction list etc. of the content provider 101 etc. handling the related content data C from the EMD service center 102.

10            In addition, for example, when the EMD service center 102 receives the content ID etc. from the user, the information specifying the related user may be notified to the content provider 101 providing the content data C corresponding to the related content ID. In this case, the content provider 101 receiving the  
15    related communication transmits the related content data C to the network apparatus of the user if the related user is a contracting subscriber or may transmit promotional information concerning itself to the network apparatus of the user if the related user is not a  
20    contracting subscriber.

          Note that, in the second embodiment mentioned later, an EMD service center 302 can introduce a service provider 310 handling the related content data C to the user based on the link watermark WL.

25            Also, in the present embodiment, preferably, the

content and buried location of each electronic watermark information are defined as a watermark module WM, and the watermark module WM is registered and managed in the EMD service center 102. The watermark module WM is used when  
5 for example the network apparatus 160<sub>1</sub> and the AV apparatuses 160<sub>2</sub> to 160<sub>4</sub> in the user home network 103 verify the legitimacy of the electronic watermark information.

For example, in the user home network 103, by  
10 deciding that the electronic watermark information is legitimate where both of the buried location of the electronic watermark information and the content of the buried electronic watermark information match based on the user watermark module managed by the EMD service  
15 center 102, the burial of a false electronic watermark information can be detected with a high probability.

The compression unit 113 compresses the content data S112 by an acoustic compression method, for example ATRAC3 (Adaptive Transform Acoustic Coding 3)  
20 (trademark), and outputs compressed content data S113 to the encryption unit 114.

In this case, at the time of compression by the compression unit 113, it is also possible to bury the electronic watermark information in the content data  
25 again. Concretely, as shown in Fig. 3, when the content

data 113 is expanded at the expansion unit 116 to produce content data S116 and the content data S116 is reproduced at the audial check unit 123, the influence exerted upon the quality of sound by the burial of the electronic watermark information is decided by for example a person actually listening to it. Where it does not satisfy a predetermined standard, the electronic watermark information addition unit 112 is instructed to perform the processing for burying the electronic watermark information again.

By this, when employing an acoustic compression method accompanied by for example loss of data, it is possible to adequately cope with the case where the buried electronic watermark information is lost due to the related compression. Further, it is also possible to expand the compressed content data again and confirm whether or not the buried electronic watermark information can be correctly detected. In this case, the feeling of the sound quality is also verified. Where there is a problem in the sound, the burial of the electronic watermark information is adjusted. For example, where the electronic watermark information is buried by using a masking effect, the layer for burying the electronic watermark information is adjusted.

The encryption unit 114 uses the content key data Kc

as the common key, encrypts the content data S113 by a common key encryption method such as DES (Data Encryption Standard) or Triple DES to produce the content data C, and outputs this to the secure container preparation unit

5 118.

Also, the encryption unit 114 encrypts an A/V expansion use software Soft, a meta data Meta, and the watermark module WM by using the content key data Kc as the common key and then outputs them to the secure  
10 container preparation unit 117.

DES is the encryption method for processing 64 bits of plain text as one block by using a common key of 56 bits. The processing of DES is comprised of a portion for scrambling the plain text to convert the same to  
15 encrypted text (data scrambling portion) and a portion for creating the key (magnification key) data used in the data scrambling portion from the common key data (key processing portion). All algorithms of the DES are public, therefore, here, the basic processing of the data  
20 scrambling portion will be simply explained.

First, 64 bits of the plain text are divided to  $H_0$  of the upper significant 32 bits and  $L_0$  of lower significant 32 bits. By receiving as input the magnification key data  $K_1$  of 48 bits supplied from the  
25 key processing unit and the  $L_0$  of the lower significant

32 bits, the output of an F function scrambled  $L_0$  of the lower significant 32 bits is calculated. The F function is comprised of two types of basic transforms of "substitution" of switching numerical values by a

5 predetermined rule and "transposition" of switching bit locations by a predetermined rule. Next, an exclusive OR of the  $H_0$  of the upper significant 32 bits and the output of the F function is calculated, and the result thereof is defined as  $L_1$ . Also,  $L_0$  is made  $H_1$ .

10 Then, based on the  $H_0$  of the upper significant 32 bits and the  $L_0$  of the lower significant 32 bits, the above processing is repeated 16 times. The obtained  $H_{16}$  of the upper significant 32 bits and  $L_{16}$  of the lower significant 32 bits are output as the encrypted text. The  
15 decryption is realized by inversely following the sequence by using the common key data used for the encryption.

The random number generation unit 115 generates a random number of a predetermined number of bits and  
20 stores the related random number as the content key data  $K_c$  in the storage unit 119.

Note that, it is also possible if the content key data  $K_c$  is produced from the information concerning a song provided by the content data. The content key data  
25  $K_c$  is updated for example every predetermined time.

Also, where a plurality of content providers 101 exist, it is also possible to use inherent content key data  $K_c$  from individual content providers 101 or it is also possible to use the content key data  $K_c$  common to  
5 all content providers 101.

In the key file database 118b, as shown in Fig. 4, the key file KF shown in Fig. 5B received from the EMD service center 102 via the EMD service center management unit 125 is stored. The key file KF exists for every  
10 content data C. As will be mentioned later, a link is designated with the corresponding content file CF by directory structure data DSD in the header of the content file CF.

In the key file KF, as shown in Fig. 5B and Fig. 7,  
15 the header, content key data  $K_c$ , usage control policy data 106 (usage permission condition) 106, SAM program download containers  $SDC_1$  to  $SDC_3$ , and signature data  $SIG_{K1,ESC}$  are stored.

Here, as the signature data using the secret key  
20 data  $K_{ESC,S}$  of the content provider 101, use can be also made of the signature data  $K_{1,ESC}$  for all data stored in the key file KF as shown in Fig. 5B. Alternatively, signature data for the data from the header to the information concerning the key file, signature data for  
25 the content key data  $K_c$  and the usage control policy data



106, and signature data for the SAM program download container SDC can be separately provided too as shown in Fig. 7.

The content key data  $K_c$  and usage control policy data 106 and the SAM program download containers  $SDC_1$  to  $SDC_3$  are encrypted by using the distribution use key data  $KD_1$  to  $KD_6$  of the corresponding periods.

In the header data, as shown in Fig. 7, a synchronization signal, the content ID, the signature data by the secret key data  $K_{ESC,S}$  of the content provider 101 for the content ID, the directory structure data, hyper link data, the information concerning the key file KF, the signature data by the secret key data  $K_{ESC,S}$  of the content provider 101 for the directory structure data, etc. are contained.

Note that, as the information to be contained in the header data, various information can be considered and freely varied according to the situation. For example, it is also possible if the information as shown in Fig. 8 is contained in the header data.

Also, in the content ID, for example, the information as shown in Fig. 9 is contained. The content ID is produced in the EMD service center 102 or the content provider 101. Where it is produced in the EMD service center 102, the signature data by the secret key

data  $K_{ESC,S}$  of the EMD service center 102 is added as shown in Fig. 9, while where it is produced at the content provider 101, the secret key data  $K_{CP,S}$  of the content provider 101 is added.

5       The content ID is produced by for example the content ID generation unit 850 as shown in Fig. 4 and stored in the storage unit 119. Note that, it is also possible if the content ID is produced by the EMD service center 102.

10       The directory structure data indicates correspondence among the content files CF in the secure container 104 and correspondence between the content files CF and the key files KF.

For example, where the content files  $CF_1$  to  $CF_3$  and  
15   the key files  $KF_1$  to  $KF_3$  corresponding to them are stored in the secure container 104, as shown in Fig. 10, the links among the content files  $CF_1$  to  $CF_3$  and the links between the content files  $CF_1$  to  $CF_3$  and the key files  $KF_1$  to  $KF_3$  are established by the directory structure data.

20       The hyper link data indicates a hierarchy structure among the key files KF and the correspondence between the content files CF and the key files KF covering all files inside and outside the secure container 104.

Concretely, as shown in Fig. 11, the address  
25   information of the linked site for every content file CF

and key file KF and the certificate value (hash value) thereof are stored in the secure container 104. The links are verified by comparing the hash value of one's own address information obtained by using the hash function  $H(x)$  and the certificate value of the other party.

Also, in the usage control policy data 106, as shown in Fig. 7, the content ID, identifier CP\_ID of the content provider 101, an expiration date of the usage control policy data 106, the communication address of the EMD service center 102, usage space examination information, wholesale price information, a handling plan, handling control information, handling control information of a commodity demo, the signature data for them, etc. are contained.

Note that, as in the second embodiment mentioned later, where a secure container 304 is transmitted via the service provider 310 to a user home network 303, in the usage control policy data 106, an identifier SP\_ID of the service provider 310 for providing the secure container 104 by the content provider 301 is contained.

Also, in the SAM program download containers SDC<sub>1</sub> to SDC<sub>3</sub>, as shown in Fig. 7, a download driver indicating the routine of the download used when downloading a program in the SAMs 105<sub>1</sub> to 105<sub>4</sub>, a label reader such as

an UCP-L (Label) R (Reader) indicating a syntax (grammar) of the usage control policy data (UCP) U106, lock key data for locking/unlocking rewriting and erasing of the storage units (flash-ROM) built in the SAMs 105<sub>1</sub> to 105<sub>4</sub> in block units, and the signature data for them are contained.

Note that, the storage unit 119 is provided with various databases including for example a database for storing the certificate data.

10       The signature processing unit 117 obtains the hash value of the data covered by the signature and produces the signature data SIG thereof by using the secret key data  $K_{CP,S}$  of the content provider 101.

15       Note that, the hash value is produced by using a hash function. A hash function is a function receiving as input the data covered, compressing the related input data to data having a predetermined bit length, and outputting the same as the hash value. The hash function has as its characteristic feature that it is difficult to predict the input of the hash function from the hash value (output). When one bit input to the hash function varies, many bits of the hash value vary, so it is difficult to find the input data having an identical hash value.

25       The secure container preparation unit 118 produces

the content file CF storing the header data, meta data  
Meta, the content data C, A/V expansion use software  
Soft, and the watermark module WM input from the  
encryption unit 114 and encrypted by the content key data  
5 Kc therein as shown in Fig. 5A.

It is also possible to contain the file reader and  
the signature data of the file reader in the secret key  
data  $K_{CP,S}$  as shown in Fig. 6. By doing this, in the SAMs  
105<sub>1</sub> to 105<sub>4</sub>, a plurality of secure containers 104  
10 storing the content files CF of different formats  
received from a plurality of secure containers 104 of  
different streams can be efficiently processed.

Here, the file reader is used when reading a content  
file CF and the key file KF corresponding to that and  
15 indicates the reading routine etc. of these files.

Note, in the present embodiment, a case where the  
related file reader is transmitted in advance from the  
EMD service center 102 to the SAMs 105<sub>1</sub> to 105<sub>4</sub> is  
exemplified. Namely, in the present embodiment, the  
20 content file CF of the secure container 104 does not  
store the file reader.

In the header data, as shown in Fig. 6, the  
synchronization signal, content ID, signature data by the  
secret key data  $K_{CP,S}$  of the content provider 101 for the  
25 content ID, directory information, hyper link

information, serial number, expiration date and producer  
information of the content file CF, file size, existence  
of encryption, encryption algorithm, information  
concerning the signature algorithm, signature data by the  
5 secret key data  $K_{CP,S}$  of the content provider 101  
concerning the directory information, etc. are contained.

In the meta data Meta, as shown in Fig. 6,  
explanatory text of the commodity (content data C),  
commodity demo and PR information, information related to  
10 the commodity, and the signature data from the content  
provider 101 for them are contained.

In the present invention, as shown in Fig. 5 and  
Fig. 6, the case where the meta data Meta is stored in  
the content file CF and transmitted is exemplified, but  
15 it is also possible not to store the meta data Meta in  
the content file CF, but transmit the same from the  
content provider 101 to the SAM 105<sub>1</sub> etc. through a route  
different from the route for transmitting the content  
file CF.

20 The A/V expansion use software Soft is the software  
used when expanding the content file CF in the network  
apparatus 160<sub>1</sub> and the AV apparatuses 160<sub>2</sub> to 160<sub>4</sub> of the  
user home network 103 and is the expansion use software  
of for example the ATRAC3 method.

25 In this way, by storing the A/V expansion use

software Soft in the secure container 104, the content data C can be expanded by using the A/V expansion use software Soft stored in the secure container 104 in the SAMs 105<sub>1</sub> to 105<sub>4</sub>. Even if the compression and expansion method of the content data C is freely set by the content provider 101 for every content data C or every content provider 101, a large load will not be imposed on the user.

The watermark module WM contains for example the information required for detecting the electronic watermark information buried in the content data C and software as mentioned before.

Also, the secure container preparation unit 118 produces the secure container 104 storing the content file CF shown Fig. 5A mentioned above, signature data SIG<sub>6,CP</sub> of the related content file CF, the key file KF shown in Fig. 5B corresponding to the related content file CF read out from the key file database 118b, signature data SIG<sub>7,CP</sub> of the related key file KF, certificate data CER<sub>CP</sub> of the content provider 101 read out from the storage unit 119, and signature data SIG<sub>1,ESC</sub> of the related certificate data CER<sub>CP</sub> therein.

Here, the signature data SIG<sub>6,CP</sub> is used for verifying the legitimacy of the producer and transmitter of the content file CF at the received site of the secure

container 104.

Here, the signature data  $SIG_{7,CP}$  is used for verifying the legitimacy of the transmitter of the key file KF at the received site of the secure container 104.

5 Note that, at the received site of the secure container 104, the legitimacy of the producer of the key file KF is verified based on the signature data  $SIG_{K1,ESC}$  in the key file KF. Also, the signature data  $SIG_{K1,ESC}$  is used also for verifying whether or not the key file KF is  
10 registered in the EMD service center 102.

In the present embodiment, the encrypted content data C is stored in the secure container 104 in a form not depending upon the compression method of the content data C, existence of compression, encryption method  
15 (including both the cases of the common key encryption method and public key encryption method), parameters of the signals giving the content data C (sampling frequency etc.), and the preparation method (algorithm) of the signature data. Namely, these items can be freely  
20 determined by the content provider 101.

Also, the secure container preparation unit 118 outputs the secure container 104 stored in the secure container database 118a to the SAM management unit 124 in response to a request from the user.

25 In this way, in the present embodiment, an in-band



method of storing the certificate  $CER_{CP}$  of the public key data  $K_{CP,P}$  of the content provider 101 in the secure container 104 and transmitting the same to the user home network 103 is employed. Accordingly, the user home  
5 network 103 does not have to communicate with the EMD service center 102 for obtaining the certificate  $CER_{CP}$ .

Note that, in the present invention, it is also possible to employ an out-of-band method of obtaining the certificate  $CER_{CP}$  from the EMD service center 102 by the  
10 user home network 103 without storing the certificate  $CER_{CP}$  in the secure container 104.

The mutual certification unit 120 performs mutual certification between the EMD service center 102 and the user home network 103 to produce the session key data  
15 (common key)  $K_{SES}$  when the content provider 101 transmits or receives data on-line with the EMD service center 102 and the user home network 103. The session key data  $K_{SES}$  is newly produced at each mutual certification.

The encryption and/or decryption unit 121 encrypts  
20 the data to be transmitted on-line to the EMD service center 102 and the user home network 103 by the content provider 101 by using the session key data  $K_{SES}$ .

Also, the encryption and/or decryption unit 121 decrypts the data received on-line from the EMD service  
25 center 102 and the user home network 103 by the content

provider 101 by using the session key data  $K_{SES}$ .

The usage control policy data preparation unit 122 produces the usage control policy data 106 and outputs this to the EMD service center management unit 125.

5       The usage control policy data 106 is a descriptor defining operating rules of the content data C and for example describes the suggested retailer's price SRP intended by an operator of the content provider 101, copy rule of the content data C, etc.

10       The SAM management unit 124 supplies the secure container 104 off-line or on-line to the user home network 103.

Also, when distributing the secure container 104 to the SAMs 105<sub>1</sub> to 105<sub>4</sub> on-line, the SAM management unit  
15   124 uses, as the communication protocol for transmitting the secure container 104, an MHEG (Multimedia and Hypermedia Information Coding Experts Group) protocol if a digital broadcast or uses an XML/SMIL/HTML (Hyper  
20   TextMarkup Language) if the Internet and buries the secure containers 104 in these communication protocols in a form not depending upon the coding method by tunneling.

Accordingly, it is not necessary to match formats between the communication protocol and the secure container 104, so the format of the secure container 104  
25   can be flexibly set.

Note that, the communication protocol used when transmitting the secure container 104 from the content provider 101 to the user home network 103 is not limited to those mentioned above and may be any protocol.

5        Figure 12 is a view for explaining a storage medium 130<sub>1</sub> of a ROM type used in the present embodiment.

As shown in Fig. 12, the ROM type storage medium 130<sub>1</sub> has a ROM region 131, a secure RAM region 132, and a media SAM 133.

10        In the ROM region 131, the content file CF shown in Fig. 5A is stored.

Also, the secure RAM region 132 is a region where predetermined permission (certification) is necessary for accessing the stored data. Signature data produced by  
15        using a MAC (Message Authentication Code) function with the key file KF and the certificate data CER<sub>CP</sub> and a storage use key data K<sub>STR</sub> having an inherent value in accordance with the type of the apparatus shown in Figs. 5B and 5C as factors and the data obtained by encrypting  
20        the related key file KF and the certificate data CER<sub>CP</sub> by using media key data K<sub>MED</sub> having an inherent value in the storage medium are stored.

Also, in the secure RAM region 132, for example, certificate revocation data (revocation list) for  
25        specifying the content provider 101 and the SAMs 105<sub>1</sub> to

105<sub>5</sub>, which became invalid due to illegitimate actions or the like is stored.

Also, in the secure RAM region 132, as will be mentioned later, usage control status (UCS) data 166 etc. produced when the purchase and/or usage form of the content data C is determined in the SAMs 105<sub>1</sub> to 105<sub>4</sub> of the user home network 103 is determined are stored. By this, by the storage of the user control status data 166 in the secure RAM region 132, a ROM type storage medium 130 with a purchase and/or usage form determined therein is obtained.

In the media SAM 133, for example the media ID serving as the identifier of the ROM type storage medium 130<sub>1</sub> and the media key data  $K_{MED}$  are stored.

The media SAM 133 has for example a mutual certificate authority function.

As the storage medium of the ROM type used in the present embodiment, for example, other than one shown in Fig. 12, also a ROM type storage medium 130<sub>2</sub> shown in Fig. 13 and a ROM type storage medium 130<sub>3</sub> shown in Fig. 14 can be considered.

The ROM type storage medium 130<sub>2</sub> shown in Fig. 13 has the ROM region 131 and the media SAM 133 having the certificate authority function, but is not provided with the secure RAM region 132 as in the ROM type storage

medium 130<sub>1</sub> shown in Fig. 12. Where use is made of the ROM type storage medium 130<sub>2</sub>, the content file CF is stored in the ROM region 131, and the key file KF is stored in the media SAM 133.

5       Also, the ROM type storage medium 130<sub>3</sub> shown in Fig. 14 has the ROM region 131 and the secure RAM region 132 and does not have the media SAM 133 as in the ROM type storage medium 130<sub>1</sub> shown in Fig. 12. Where the ROM type storage medium 130<sub>3</sub> is used, the content file CF is  
10       stored in the ROM region 131, and the key file KF is stored in the secure RAM region 132. Also, where the ROM type storage medium 130<sub>3</sub> is used, mutual certification is not carried out with the SAM.

      Also, in the present embodiment, other than the ROM  
15       type storage medium, also a RAM type storage medium is used.

      As the RAM type storage medium used in the present embodiment, there is, for example, as shown in Fig. 15, a RAM type storage medium 130<sub>4</sub> having the media SAM 133,  
20       secure RAM region 132, and nonsecure RAM region 134. In the RAM type storage medium 130<sub>4</sub>, the media SAM 133 has the certificate authority function and stores the key file KF. Also, in the RAM region 134, the content file CF is stored.

25       Also, as the RAM type storage medium used in the

present embodiment, other than that, also a RAM type storage medium 130<sub>5</sub> shown in Fig. 16 and a RAM type storage medium 130<sub>6</sub> shown in Fig. 17 can be considered.

The RAM type storage medium 130<sub>5</sub> shown in Fig. 16 has the nonsecure RAM region 134 and the media SAM 133 having the certificate authority function, but is not provided with the secure RAM region 132 as in the RAM type storage medium 130<sub>4</sub> shown in Fig. 15. Where the RAM type storage medium 130<sub>5</sub> is used, the content file CF is stored in the RAM region 134, and the key file KF is stored in the media SAM 133.

Also, the RAM type storage medium 130<sub>6</sub> shown in Fig. 17 has the secure RAM region 132 and the nonsecure RAM region 134, but does not have the media SAM 133 as in the RAM type storage medium 130<sub>4</sub> shown in Fig. 15. Where use is made of the RAM type storage medium 130<sub>6</sub>, the content file CF is stored in the RAM region 134, and the key file KF is stored in the secure RAM region 132. Also, where use is made of the RAM type storage medium 130<sub>6</sub>, mutual certification is not carried out with the SAM.

Also, where the secure container 104 is distributed on-line to the user home network 103 by using a network or a digital broadcast, the SAM management unit 124 encrypts the secure container 104 by using the session key data  $K_{SES}$  in the encryption and/or decryption unit

121, and then distributes the same via the network to the user home network 103.

In the present embodiment, as the SAM management unit and the EMD service center management unit and the content provider management unit and service provider management unit mentioned later, use is made of a communication gateway having a tamper resistant structure whereby for example monitoring and tampering of the processing content of the internal portion cannot be carried out or are difficult.

Here, in both of the case where the content data C is distributed from the content provider 101 to the user home network 103 by using the storage medium 130<sub>1</sub> and the case where it is distributed on-line by using the network, use is made of the secure container 104 of a common form with the usage control policy data 106 stored therein. Accordingly, in the SAMs 105<sub>1</sub> to 105<sub>4</sub> of the user home network 103, the rights clearing based on the common usage control policy data 106 can be carried out in both of the cases of off-line and on-line.

Also, as mentioned above, in the present embodiment, the in-band method of enclosing the content data C encrypted by the content key data Kc and the content key data Kc for decrypting the related encryption in the secure container 104 is employed. In the in-band method,

when it is intended to reproduce the content data C by the apparatus of the user home network 103, it is not necessary to separately distribute the content key data Kc, so there is an advantage that the load of the network communication can be reduced. Also, the content key data Kc has been encrypted by the distribution use key data KD<sub>1</sub> to KD<sub>6</sub>, but the distribution use key data KD<sub>1</sub> to KD<sub>6</sub> are managed at the EMD service center 102 and distributed to the SAMs 105<sub>1</sub> to 105<sub>5</sub> of the user home network 103 in advance (when the SAMs 105<sub>1</sub> to 105<sub>4</sub> access the EMD service center 102 for the first time), therefore, in the user home network 103, the usage of the content data C off-line becomes possible without connecting with the EMD service center 102 on-line.

Note that, the present invention has the flexibility to employ the out-of-band method for separately supplying the content data C and the content key data Kc to the user home network 103 as will be mentioned later.

When receiving the settlement report data 107 from the EMD service center 102, the EMD service center management unit 125 decrypts it at the encryption and/or decryption unit 121 by using the session key data K<sub>SES</sub> and then stores the same in the storage unit 119.

As the settlement report data 107, for example, the content of the settlement concerning the content provider



101 performed by the EMD service center 102 at the settlement manager 91 shown in Fig. 1 is described.

Also, the EMD service center management unit 125 transmits the content ID as a global unique identifier of the content data C to be provided, a public key data  $K_{CP,P}$ , and signature data  $SIG_{9,CP}$  of them to the EMD service center 102 and receives as input the certificate data  $CER_{CP}$  of the public key data  $K_{CP,P}$  from the EMD service center 102.

Also, the EMD service center management unit 125 produces, as shown in Fig. 18, a registration module  $Mod_2$  storing the content ID as the global unique identifier of the content data C to be provided, the content key data  $K_c$ , the usage control policy data 106, the watermark module WM,  $CP\_ID$  as the global unique identifier of the content provider 101, and signature data  $SIG_{M1,CP}$  by the secret key data  $K_{CP,S}$  of the content provider 101 for them therein when registering the content key data  $K_c$ , the usage control policy data 106, and the watermark module WM in the EMD service center 102 and receiving the key file KF for each of the content data C. Then, the EMD service center 125 encrypts the registration module  $Mod_2$  in the encryption and/or decryption unit 121 by using the session key data  $K_{SES}$  and then transmits the same via the network to the EMD service center 102. As the EMD service

center management unit 125, as mentioned above, for example use is made of a communication gateway having a high tamper resistant structure whereby monitoring or tampering of the processing content of the internal  
5 portion cannot be carried out or are difficult.

Below, an explanation will be given of the flow of the processing in the content provider 101 by referring to Fig. 3 and Fig. 4.

Note that, as a prerequisite for performing the  
10 following processing, the interested party of the content provider 101 performs the registration processing for the EMD service center 102 off-line by using for example its own ID and a bank account for performing the settlement processing and acquires the global unique identifier  
15 CP\_ID. The identifier CP\_ID is stored in the storage unit 119.

First, an explanation will be given of the processing where the content provider 101 requests the certificate data  $CER_{CP}$  for proving the legitimacy of the  
20 public key data  $K_{CP,S}$  corresponding to its own secret key data  $K_{CP,S}$  from the EMD service center 102 by referring to Fig. 4.

The content provider 101 generates a random number by using a true random number generator to produce the  
25 secret key data  $K_{CP,S}$ , produces the public key data  $K_{CP,P}$

corresponding to the related secret key data  $K_{CP,S}$  and stores the same in the storage unit 119.

The EMD service center management unit 125 reads out the identifier  $CP\_ID$  and the public key data  $K_{CP,P}$  of the content provider 101 from the storage unit 119.

Then, the EMD service center management unit 125 transmits the identifier  $CP\_ID$  and the public key data  $K_{CP,P}$  to the EMD service center 102.

Then, the EMD service center management unit 125 receives as input the certificate data  $CER_{CP}$  and the signature data  $SIG_{1,ESC}$  thereof from the EMD service center 102 in accordance with the related registration and writes them into the storage unit 119.

Next, an explanation will be given of the processing where the content provider 101 registers the content key data  $K_C$ , usage control policy data 106, and the watermark module  $WM$  in the EMD service center 102 and receives the key file  $KF$  corresponding to the content data  $C$  by referring to Fig. 4, Fig. 18, and Fig. 19.

The registration of the usage control policy data 106 etc. is carried out for individual content data  $C$ .

Figure 19 is a flowchart for explaining the registration processing from the content provider 101 to the EMD service center 102.

Step A1: Mutual certification is carried out between

the mutual certification unit 120 of the content provider 101 shown in Fig. 4 and the EMD service center 102.

Step A2: The session key data  $K_{SES}$  obtained by the mutual certification performed at step A1 is shared by  
5 the content provider 101 and the EMD service center 102.

Step A3: The content provider 101 reads out the content ID, content key data  $K_c$ , usage control policy data 106, watermark module WM, and CP\_ID, etc. to be registered into the EMD service center 102 from the  
10 database of the storage unit 119 etc.

Step A4: In the signature processing unit 117, the signature data  $SIG_{M1,CP}$  indicating the legitimacy of the sender is produced for a module containing for example the usage control policy data 106 read out at step A3 by  
15 using the secret key data  $K_{CP,S}$  of the content provider 101.

Then, the EMD service center management unit 125 produces the registration use module  $Mod_2$  storing the content ID, content key data  $K_c$ , usage control policy  
20 data 106, watermark module WM and CP\_ID, and the signature data  $SIG_{M1,CP}$  for them therein as shown in Fig. 18.

Step A5: The encryption and/or decryption unit 121 encrypts the registration use module  $Mod_2$  produced at  
25 step A4 by using the session key data  $K_{SES}$  shared at step

A2.

Step A6: The EMD service center management unit 125 transmits the registration use module  $\text{Mod}_2$  encrypted at step A5 to the EMD service center 102.

5        The processing of step A7 and following processing are the processing in the EMD service center 102.

Step A7: The EMD service center 102 decrypts the received registration use module  $\text{Mod}_2$  by using the session key data  $K_{\text{SES}}$  shared at step A2.

10       Step A8: The EMD service center 102 verifies the signature data  $\text{SIG}_{\text{M1,CP}}$  stored in the decrypted registration use module  $\text{Mod}_2$  by using the public key data  $K_{\text{CP,P}}$ , confirms the legitimacy of the sender of the registration use module  $\text{Mod}_2$ , and performs the processing  
15 of step A9 under the condition that the legitimacy of the sender is proved.

Step A9: The EMD service center 102 stores and registers the content ID, content key data  $K_c$ , usage control policy data 106, watermark module WM, and CP\_ID  
20 stored in the registration use module  $\text{Mod}_2$  in the predetermined database.

Note that, the EMD service center management unit 125 receives, as shown in Fig. 18, for example six months' worth of the key files KF from the EMD service  
25 center 102 after the registration processing in

accordance with the registration use module  $\text{Mod}_2$  is carried out for the EMD service center 102, decrypts the related received key files KF by using the session key data  $K_{\text{SES}}$  obtained by the mutual certification between the mutual certification unit 120 and the EMD service center 102, and then stores the same in the key file database 118b.

Next, an explanation will be given of the processing where the content provider 101 transmits the secure container 104 to the SAM 105<sub>1</sub> of the user home network 103 by referring to Fig. 3 and Fig. 4.

Note that, in the following example, the case where the secure container 104 is transmitted from the content provider 101 to the SAM 105<sub>1</sub> is exemplified, but the case where the secure container 104 is transmitted to each of the SAMs 105<sub>2</sub> to 105<sub>4</sub> is the same except it transmitted to each of the SAMs 105<sub>2</sub> to 105<sub>4</sub> via the SAM 105<sub>1</sub>.

First, as shown in Fig. 3, the content data S111 is read out from the content master source database 111 and output to the electronic watermark information addition unit 112.

Next, the electronic watermark information addition unit 112 buries the electronic watermark information in the content data S111 to produce the content data S112 and outputs this to the compression unit 113.

Next, the compression unit 113 compresses the content data S112 by for example the ATRAC3 method to produce the content data S113 and outputs this to the encryption unit 114.

5       Also, as shown in Fig. 4, the content key data Kc is produced by generating a random number at the random number generation unit 115, and the related produced content key data Kc is stored in the storage unit 119.

10       Next, the encryption unit 114 encrypts the content data S113 input from the compression unit 113, meta data Meta read out from the storage unit 119, the A/V expansion use software Soft and the watermark module WM by using the content key data Kc and outputs the same to the secure container preparation unit 118. In this case,  
15       it is also possible if the meta data Meta and the watermark module WM are not encrypted.

Then, the secure container preparation unit 118 produces the content file CF shown in Fig. 5A. Also, in the signature processing unit 117, the hash value of the  
20       content file CF is obtained and the signature data  $SIG_{6,CP}$  is produced by using the secret key data  $K_{CP,S}$ .

Also, the secure container preparation unit 118 reads out the key file KF corresponding to the content data C from the key file database 118b and outputs this  
25       to the signature processing unit 117.

Then, the signature processing unit 117 obtains the hash value of the key file KF input from the secure container preparation unit 118, produces the signature data  $SIG_{7,CP}$  by using the secret key data  $K_{CP,S}$ , and outputs  
5 this to the secure container preparation unit 118.

Next, the secure container preparation unit 118 produces the secure container 104 storing the content file CF and the signature data  $SIG_{6,CP}$  thereof shown in Fig. 5A, the key file KF and the signature data  $SIG_{7,CP}$   
10 thereof shown in Fig. 5B, and the certificate data  $CER_{CP}$  and the signature data  $SIG_{1,ESC}$  thereof shown in Fig. 5C read out from the storage unit 119 therein and stores this in the secure container database 118b. Then, the secure container preparation unit 118 reads out the  
15 secure container 104 to be provided to the user home network 103 in response to for example a request from the user from the secure container database 118a, encrypts this at the encryption and/or decryption unit 121 by using the session key data  $K_{SES}$  obtained by the mutual  
20 certification between the mutual certification unit 120 and the SAM 105<sub>1</sub>, and then transmits the same via the SAM management unit 124 to the SAM 105<sub>1</sub> of the user home network 103.

Below, a summary of the flow of the overall  
25 processing of the content provider 101 will be explained



relative to the secure container preparation processing.

Figure 20, Fig. 21, and Fig. 22 are flowcharts for explaining the flow of the related processing.

Step B1: The content provider 101 receives as input  
5 its own certificate data  $CER_{CP}$  from the EMD service  
center 102 in advance and stores this in the storage unit  
(database) 119.

Step B2: The content data to be newly authored and  
an already stored content master source such as legacy  
10 content data are digitized, allocated a content ID, and  
stored in the content master source database 111 and  
uniquely managed.

Step B3: The meta data Meta is produced for each  
content master source uniquely managed at step B1 and is  
15 stored in the storage unit 119.

Step B4: The content data S111 serving as the  
content master source is read out from the content master  
source database 111 and output to the electronic  
watermark information addition unit 112, the electronic  
20 watermark information is buried, and the content data  
S112 is produced.

Step B5: The electronic watermark information  
addition unit 112 stores the content of the buried  
electronic watermark information and the burial location  
25 in the predetermined database.

Step B6: In the compression unit 113, the content data S112 with the electronic watermark information buried therein is compressed to produce the content data S113.

5 Step B7: In the expansion unit 116, the compressed content data S113 is expanded to produce the content data S116.

10 Step B8: In the audial check unit 123, the check of the sound of the expanded content data S116 is carried out.

Step B9: The content provider 101 detects the electronic watermark information buried in the content data S116 based on the buried content and the burial location stored in the database at step B5.

15 Then, the content provider 101 performs the processing of step B10 where both of the audial check and the detection of the electronic watermark information succeed, while repeats the processing of step B4 where either one fails.

20 Step B10: A random number is generated at the random number generation unit 115 to produce the content key data Kc, and this is stored in the storage unit 119.

Step B11: In the encryption unit 114, the compressed content data S113 is encrypted by using the content key data Kc to produce the content data C.

25

Step B12: In the usage control policy data preparation unit 122, the usage control policy data 106 for the content data C is produced.

Step B13: The content provider 101 determines the SRP and stores this in the storage unit 119.

Step B14: The content provider 101 outputs the content ID, content key data  $K_c$ , and the usage control policy data 106 to the EMD service center 102.

Step B15: The content provider 101 receives as input the key file KF encrypted by the distribution use key data  $KD_1$  to  $KD_3$  from the EMD service center 102.

Step B16: The content provider 101 stores the input key file KF in the key file database 118b.

Step B17: The content provider 101 connects the links of the content data C and the key file KF by the hyper link.

Step B18: In the signature processing unit 117, the signature data indicating the legitimacy of the producer is produced by using the secret key data  $K_{CP,S}$  for each of the content data C and the key files KF.

Step B19: In the secure container preparation unit 118, the secure container 104 shown in Fig. 5 is produced.

Step B20: Where the content data is provided in a composite form using a plurality of secure containers,

the processing of the steps B1 to B19 is repeated to produce the secure container 104 and the link between the content file CF and the key file KF and the link among the content files CF by using the hyper link, etc.

5       Step B21: The content provider 101 stores the produced secure container 104 in the secure container database 118a.

[EMD service center 102]

10       The EMD service center 102 has a certificate authority (CA) function, a key management function, and a rights clearing (profit distribution) function.

Figure 23 is a view of the configurations of functions of the EMD service center 102.

As shown in Fig. 23, the EMD service center 102 has  
15   a key server 141, a key database 141a, a settlement processing unit 142, a signature processing unit 143, a settlement manager management unit 144, a certificate and/or usage control policy management unit 145, a usage control policy database 145a, a certificate database  
20   145b, a content provider management unit 148, a CP database 148a, a SAM management unit 149, a SAM database 149a, a mutual certification unit 150, an encryption and/or decryption unit 151, and a KF preparation unit 153.

25       Note that, in Fig. 23, the flow of the data related

to the data transmitted and received between the EMD service center 102 and the content provider 101 in the flow of the data among the functional blocks in the EMD service center 102 is shown.

5       Also, in Fig. 24, the flow of the data related to the data transmitted and received between the SAMs 105<sub>1</sub> to 105<sub>4</sub> and the settlement manager 91 shown in Fig. 1 in the flow of the data among the functional blocks in the EMD service center 102 is shown.

10       The key server 141 reads out six months' worth of the distribution use key data having the expiration date of one month stored in the key database 141a and outputs the same to the SAM management unit 149.

15       Also, other than the key database 141a distribution use key data KD, one series of key data for storing the key data such as the secret key data  $K_{ESC,S}$  of the EMD service center 102, storage use key data  $K_{STR}$ , media key data  $K_{MED}$ , and the MAC key data  $K_{MAC}$  are stored.

20       The settlement processing unit 142 performs settlement processing based on the usage log data 108 input from the SAMs 105<sub>1</sub> to 105<sub>4</sub>, the suggested retailer's price SRP input from the certificate and/or usage control policy management unit 145 and sales price, produces the settlement report data 107 and settlement  
25       claim data 152, outputs the settlement report data 107 to

the content provider management unit 148, and outputs the settlement claim data 152 to the settlement manager management unit 144.

Note that, the settlement processing unit 142  
5 monitors whether or not transactions based on an illegal dumping price were carried out based on the sales price.

Here, the usage log data 108 indicates the log of the purchase and usage (reproduction, recording, transfer, etc.) of the secure container 104 in the user  
10 home network 103 and is used when determining the payment sum of a license fee related to the secure container 104 in the settlement processing unit 142.

In the usage log data 108, for example the content ID serving as the identifier of the content data C stored  
15 in the secure container 104, the identifier CP\_ID of the content provider 101 distributing the secure container 104, the compression method of the content data C in the secure container 104, an identifier Media\_ID of the storage medium storing the secure container 104, the  
20 identifier SAM\_ID of the SAMs 105<sub>1</sub> to 105<sub>4</sub>, receiving the distribution of the secure container 104, USER\_ID of the user of the related SAMs 105<sub>1</sub> to 105<sub>4</sub>, etc. are described. Accordingly, the EMD service center 102 determines the sum of payment for each other party based  
25 on a distribution rate table determined in advance when

it is necessary to distribute the money paid by the user of the user home network 103 to license owners of for example the compression method and the storage medium other than the owner of the content provider 101 and produces the settlement report data 107 and the settlement claim data 152 in accordance with the related determination. The related distribution rate table is produced for example for every content data stored in the secure container 104.

Also, the settlement claim data 152 is the authenticated data for which the payment of money to the settlement manager 91 may be claimed. For example, when the money paid by the user is distributed to a plurality of right holders, it is produced for individual right holders.

Note that, the settlement manager 91 sends a statement of the related settlement manager to the EMD service center 102 when the settlement is terminated. The EMD service center 102 notifies the content of the related statement to the corresponding right holders.

The settlement manager management unit 144 transmits the settlement claim data 152 produced by the settlement processing unit 142 via the payment gateway 90 shown in Fig. 1 to the settlement manager 91.

Note that, as will be mentioned later, it is also

possible if the settlement manager management unit 144 transmits the settlement claim data 152 to the right holders of the content provider 101 etc., and the right holders per se perform the settlement at the settlement  
5 manager 91 by using the received settlement claim data 152.

Also, the settlement manager management unit 144 obtains the hash value of the settlement claim data 152 in the signature processing unit 143 and transmits  
10 signature data  $SIG_{99}$ , produced by using the secret key data  $K_{ESC,S}$  together with the settlement claim data 152 to the settlement manager 91.

The certificate and/or usage control policy management unit 145 reads out the certificate data  $CER_{CP}$   
15 and certificate data  $CER_{SAM1}$  to  $CER_{SAM4}$  etc. which are registered (stored) in the certificate database 145b and authenticated and, at the same time, registers the usage control policy data 106 of the content provider 101, the content key data  $Kc$ , the watermark module  $WM$ , etc. in the  
20 usage control policy database 145a to authenticate the same.

Here, for the usage control policy database 145a, a search is carried out by using the content ID as a search key, while for the certificate database 145b, a search is  
25 carried out by using the identifier  $CP\_ID$  of the content



provider 101 as the search key.

Also, the certificate and/or usage control policy management unit 145 obtains the hash values of for example the usage control policy data 106, content key data Kc, and the watermark module WM and stores the authenticated data attached with the signature data using the secret key data  $K_{ESC,S}$  in the usage control policy database 145a.

The content provider management unit 148 has a function of communication with the content provider 101 and can access the CP database 148a for managing the identifiers CP\_ID etc. of the registered content providers 101.

The SAM management unit 149 has a function of communication with the SAMs 105<sub>1</sub> to 105<sub>4</sub> in the user home network 103 and can access the SAM database 149a storing the identifiers SAM\_ID and SAM registration list etc. of the registered SAMs.

The KF preparation unit 153 outputs the content key data Kc and usage control policy data 106 input from the content provider management unit 148 and the SAM program download containers SDC<sub>1</sub> to SDC<sub>3</sub> to the signature processing unit 143.

Also, the KF preparation unit 153 encrypts the content key data Kc, the usage control policy data 106,

and the SAM program download containers  $SDC_1$  to  $SDC_3$  by using the distribution use key data  $KD_1$  to  $KD_6$  of the corresponding period input from the key server 141, produces the key file KF storing the related encrypted data and the signature data  $SIG_{K1,ESC}$  by the secret key data  $K_{ESC,S}$  for the related encrypted data input from the signature processing unit 143 therein as shown in Fig. 5B, and stores the related produced key file KF in the KF database 153a.

Below, an explanation will be given of the flow of the processing in the EMD service center 102.

First, an explanation will be given of the flow of the processing when transmitting the distribution use key data from the EMD service center 102 to the SAMs  $105_1$  to  $105_4$  in the user home network 103 by referring to Fig. 24.

As shown in Fig. 24, the key server 141 reads out for example three months' worth of the distribution use key data  $KD_1$  to  $KD_3$  from the key database 141a every predetermined period and outputs the same to the SAM management unit 149.

Also, the signature processing unit 143 obtains the hash values of each of the distribution use key data  $KD_1$  to  $KD_3$  to produce signature data  $SIG_{KD1,ESC}$  to  $SIG_{KD3,ESC}$  individually corresponding to them by using the secret

key data  $K_{ESC,S}$  of the EMD service center 102 and outputs them to the SAM management unit 149.

The SAM management unit 149 encrypts these three months' worth of the distribution use key data  $KD_1$  to  $KD_3$  and the signature data  $SIG_{KD1,ESC}$  to  $SIG_{KD3,ESC}$  of them by using the session key data  $K_{SES}$  obtained by the mutual certification between the mutual certification unit 150 and the SAMs  $105_1$  to  $105_4$ , and then transmits them to the SAMs  $105_1$  to  $105_4$ .

Next, an explanation will be given of the processing in the case where the EMD service center 102 receives an issuance request of the certificate data  $CER_{CP}$  from the content provider 101 by referring to Fig. 23.

In this case, when receiving the identifier  $CP\_ID$  of the content provider 101, public key data  $K_{CP,P}$ , and the signature data  $SIG_{9,CP}$  from the content provider 101, the content provider management unit 148 decrypts them by using the session key data  $K_{SES}$  obtained by the mutual certification between the mutual certification unit 150 and the mutual certification unit 120 shown in Fig. 4.

Then, after confirming the legitimacy of the related decrypted signature data  $SIG_{9,CP}$  at the signature processing unit 143, it is confirmed whether or not the content provider 101 issuing the issuance request of the related certificate data is registered in the CP database

148a based on the identifier CP\_ID and the public key data  $K_{CP,P}$ .

Then, the certificate and/or usage control policy management unit 145 reads out the certificate data  $CER_{CP}$  of the related content provider 101 from the certificate database 145b and outputs this to the content provider management unit 148.

Also, the signature processing unit 143 obtains the hash value of the certificate data  $CER_{CP}$ , produces the signature data  $SIG_{1,ESC}$  by using the secret key data  $K_{ESC,S}$  of the EMD service center 102, and outputs this to the content provider management unit 148.

Then, the content provider management unit 148 encrypts the certificate data  $CER_{CP}$  and the signature data  $SIG_{1,ESC}$  thereof by using the session key data  $K_{SES}$  obtained by the mutual certification between the mutual certification unit 150 and the mutual certification unit 120 shown in Fig. 4 and then transmits the same to the content provider 101.

Next, an explanation will be given of the processing where the EMD service center 102 receives the issuance request of the certificate data  $CER_{SAM1}$  from the SAM 105<sub>1</sub> by referring to Fig. 24.

In this case, when receiving an identifier  $SAM_1\_ID$  of the SAM 105<sub>1</sub>, public key data  $K_{SAM1,P}$ , and signature

data  $SIG_{8, SAM1}$  from the SAM 105<sub>1</sub>, the SAM management unit 149 decrypts them by using the session key data  $K_{SES}$  obtained by the mutual certification between the mutual certification unit 150 and the SAM 105<sub>1</sub>.

5        Then, after confirming the legitimacy of the related decrypted signature data  $SIG_{8, SAM1}$  in the signature processing unit 143, based on the identifier  $SAM_1\_ID$  and the public key data  $K_{SAM1, P}$ , it is confirmed whether or not the SAM 105<sub>1</sub> outputting the issuance request of the  
10    related certificate data is registered in the SAM database 149a.

Then, the certificate and/or usage control policy management unit 145 reads out the certificate data  $CER_{SAM1}$  of the related SAM 105<sub>1</sub> from the certificate database  
15    145b and outputs this to the SAM management unit 149.

Also, the signature processing unit 143 obtains the hash value of the certificate data  $CER_{SAM1}$ , produces signature data  $SIG_{50, ESC}$  by using the secret key data  $K_{ESC, S}$  of the EMD service center 102, and outputs this to the  
20    SAM management unit 149.

Then, the SAM management unit 149 encrypts the certificate data  $CER_{SAM1}$  and the signature data  $SIG_{50, ESC}$  thereof by using the session key data  $K_{SES}$  obtained by the mutual certification between the mutual certification  
25    unit 150 and the SAM 105<sub>1</sub>, and then transmits the same to

the SAM 105<sub>1</sub>.

Note that, the processing where the SAMs 105<sub>1</sub> to 105<sub>4</sub> request the certificate data is the same as the case of the SAM 105<sub>1</sub> mentioned above except only the object is replaced by the SAMs 105<sub>1</sub> to 105<sub>4</sub>.

Note that, in the present invention, it is also possible if the EMD service center 102 produces the certificate data  $CER_{SAM1}$  of the public key data  $K_{SAM1,P}$  at the time of shipment when a secret key data  $K_{SAM1,S}$  and the public key data  $K_{SAM1,P}$  of the SAM 105<sub>1</sub> are stored in the storage unit of the SAM 105<sub>1</sub> at for example the related shipment of the SAM 105<sub>1</sub>.

At this time, at the related shipment, it is also possible to store the certificate data  $CER_{SAM1}$  in the storage unit of the SAM 105<sub>1</sub>.

Next, an explanation will be given of the processing where the EMD service center 102 receives the registration use module  $Mod_2$  shown in Fig. 1 from the content provider 101 by referring to Fig. 23.

In this case, when the content provider management unit 148 receives the registration use module  $Mod_2$  shown in Fig. 18 from the content provider 101, the registration use module  $Mod_2$  is decrypted by using the session key data  $K_{SES}$  obtained by the mutual certification between the mutual certification unit 150 and the mutual

certification unit 120 shown in Fig. 4.

Then, in the signature processing unit 143, the legitimacy of the signature data  $SIG_{M1,CP}$  is verified by using the public key data  $K_{CP,P}$  read out from the key database 141a.

Next, the certificate and/or usage control policy management unit 145 registers the usage control policy data 106, content key data  $K_c$ , watermark module  $WM$ , and SRP stored in the registration use module  $Mod_2$  in the usage control policy database 145a.

Next, the content provider management unit 148 outputs the content key data  $K_c$  and the usage control policy data 106 to the KF preparation unit 153.

Next, the KF preparation unit 153 outputs the content key data  $K_c$  and usage control policy data 106 input from the content provider management unit 148 and the SAM program download containers  $SDC_1$  to  $SDC_3$  to the signature processing unit 143.

Then, the signature processing unit 143 obtains the hash value with respect to the whole data input from the KF preparation unit 153, produces the signature data  $SIG_{K1,ESC}$  thereof by using the secret key data  $K_{ESC,S}$  of the EMD service center 102, and outputs this to the KF preparation unit 153.

Next, in the KF preparation unit 153, by using the

distribution use key data  $KD_1$  to  $KD_6$  of the corresponding period input from the key server 141, the content key data  $Kc$  and usage control policy data 106 and the SAM program download containers  $SDC_1$  to  $SDC_3$  are encrypted, and the key file  $KF$  storing the related encrypted data and the signature data  $SIG_{K1,ESC}$  input from the signature processing unit 143 therein is produced and is stored in the  $KF$  database 153a.

Here, as the SAM program download containers  $SDC_1$  to  $SDC_3$ , it is also possible to use those stored in the registration use module  $Mod_2$  or it is also possible to use those held by the EMD service center 102 in advance.

Next, the content provider management unit 148 encrypts the key file  $KF$  obtained by accessing the  $KF$  database 153a by using the session key data  $K_{SES}$  obtained by the mutual certification between the mutual certification unit 150 and the mutual certification unit 120 shown in Fig. 4, and then transmits the same to the content provider 101.

Next, an explanation will be given of the settlement processing performed in the EMD service center 102 by referring to Fig. 24.

When receiving as input the usage log data 108 and signature data  $SIG_{200,SAM1}$  thereof from for example the SAM 105<sub>1</sub> of the user home network 103, the SAM management



unit 149 decrypts the usage log data 108 and the signature data  $SIG_{200, SAM1}$  by using the session key data  $K_{SES}$  obtained by the mutual certification between the mutual certification unit 150 and the SAM 105<sub>1</sub>, verifies the  
5 signature data  $SIG_{200, SAM1}$  by the public key data  $K_{SAM1}$  of the SAM 105<sub>1</sub>, and then outputs the same to the settlement processing unit 142.

Then, the settlement processing unit 142 performs the settlement processing based on the usage log data 108  
10 input from the SAM management unit 149 and the suggested retailer's price SRP contained in the usage control policy data 106 read out from the usage control policy database 145a via the certificate and/or usage control policy management unit 145 and the sales price and  
15 produces the settlement claim data 152 and the settlement report data 107.

The settlement processing unit 142 outputs the settlement claim data 152 to the settlement manager management unit 144 and, at the same time, outputs the  
20 settlement report data 107 to the content provider management unit 148.

Next, the settlement manager management unit 144 transmits the settlement claim data 152 and the signature data  $SIG_{99}$  thereof via the payment gateway 90 shown in  
25 Fig. 1 to the settlement manager 91 after the mutual

certification and the decryption by the session key data  $K_{SES}$ .

By this, the money of the sum indicated in the settlement claim data 152 is paid to the content provider 101.

Next, an explanation will be given of the processing where the EMD service center 102 transmits the settlement report to the content provider 101 by referring to Fig. 23.

When the settlement is carried out in the settlement processing unit 142, as mentioned above, the settlement report data 107 is output from the settlement processing unit 142 to the content provider management unit 148.

In the settlement report data 107, as mentioned above, for example the content of the settlement concerning the content provider 101 performed with respect to the settlement manager 91 shown in Fig. 1 by the EMD service center 102 is described.

When receiving as input the settlement report data 107 from the settlement processing unit 142, the EMD service center 102 encrypts this by using the session key data  $K_{SES}$  obtained by the mutual certification between the mutual certification unit 150 and the mutual certification unit 120 shown in Fig. 4 and then transmits the same to the content provider 101.

Also, after registering (authenticating) the usage control policy data 106 as mentioned above, the EMD service center 102 may encrypt the authenticated certificate module by the distribution use key data  $KD_1$  to  $KD_6$  and transmit the same from the EMD service center 102 to the content provider 101 too.

Also, the EMD service center 102 performs the processing at the time of shipment of the SAMs  $105_1$  to  $105_4$  and the registration processing of the SAM registration list other than the above, but these processings will be mentioned later.

[User home network 103]

The user home network 103 has a network apparatus  $160_1$  and A/V apparatuses  $160_2$  to  $160_4$  as shown in Fig. 1.

The network apparatus  $160_1$  includes a built-in SAM  $105_1$ . Also, the AV apparatuses  $160_2$  to  $160_4$  includes built-in SAMs  $105_2$  to  $105_4$ .

The SAMs  $105_1$  to  $105_4$  are connected to each other via a bus 191, for example, an IEEE1394 serial interface bus.

Note that, the AV apparatuses  $160_2$  to  $160_4$  can have a network communication function too or may not have the network communication function, but utilize the network communication function of the network apparatus  $160_1$  via the bus 191.

Also, the user home network 103 can have only AV apparatuses not having the network function too.

Below, an explanation will be made of the network apparatus 160<sub>1</sub>.

5        Figure 25 is a view of the configuration of the network apparatus 160<sub>1</sub>.

As shown in Fig. 25, the network apparatus 160<sub>1</sub> has the SAM 105<sub>1</sub>, a communication module 162, a decryption and/or expansion module 163, a purchase and/or usage form  
10    determination operation unit 165, a download memory 167, a reproduction module 169, and an external memory 201.

The SAMs 105<sub>1</sub> to 105<sub>4</sub> are modules for performing the charge processing in units of content and communicate with the EMD service center 102.

15        The SAMs 105<sub>1</sub> to 105<sub>4</sub> are managed in their specifications, versions, etc. by for example the EMD service center 102. If there is a desire for mounting them by a home electric apparatus maker, they are licensed as a black box charging module for charging in  
20    units of content. For example, a home electric apparatus developer/manufacturer cannot determine the specifications inside the ICs (integrated circuits) of the SAMs 105<sub>1</sub> to 105<sub>4</sub>. The EMD service center 102 standardizes the interfaces etc. of the related ICs. They  
25    are mounted in the network apparatus 160<sub>1</sub> and the AV

apparatuses 160<sub>2</sub> to 160<sub>4</sub> according to that.

The SAMs 105<sub>1</sub> to 105<sub>4</sub> are hardware modules (IC modules etc.) having tamper resistance so that the processing contents thereof are completely sheltered from the outside, the processing contents cannot be monitored or tampered with from the outside, and the data stored inside in advance and the data being processed cannot be monitored and tampered with from the outside.

When the functions of the SAMs 105<sub>1</sub> to 105<sub>4</sub> are realized in the form of ICs, secret memories are provided inside the ICs, and secret programs and secret data are stored there. If the function of a SAM can be incorporated in any other portion of the apparatus not limited to the physical form of an IC, that portion can be defined as a SAM too.

Below, a detailed explanation will be made of the function of the SAM 105<sub>1</sub>.

Note that the SAMs 105<sub>2</sub> to 105<sub>4</sub> have basically the same functions as the SAM 105<sub>1</sub>.

Figure 26 is a view of the configuration of the function of the SAM 105<sub>1</sub>.

Note that, in Fig. 26, the flow of the data related the processing of inputting a secure container 104 from the content provider 101 and decrypting the key file KF in the secure container 104 is shown.

As shown in Fig. 26, the SAM 105<sub>1</sub> has a mutual certification unit 170, encryption and/or decryption units 171, 172, and 173, a content provider management unit 180, an error correction unit 181, a download memory management unit 182, a secure container decryption unit 183, a decryption and/or expansion module management unit 184, an EMD service center management unit 185, a usage monitor unit 186, a charge processing unit 187, a signature processing unit 189, a SAM management unit 190, a media SAM management unit 197, a stack (work) memory 200, and an external memory management unit 811.

Note that, the AV apparatuses 160<sub>2</sub> to 160<sub>4</sub> do not have the download memory 167, so the download memory management unit 182 does not exist in the SAM 105<sub>2</sub> to 105<sub>4</sub>.

Note that, the predetermined function of the SAM 105<sub>1</sub> shown in Fig. 26 is realized by executing a secret program in for example a not illustrated CPU.

Also, in the external memory 201, after going through the following processing, as shown in Fig. 27, a usage log data 108 and a SAM registration list are stored.

Here, the memory space of the external memory 201 cannot be seen from the outside (for example a host CPU 810) of the SAM 105<sub>1</sub>. Only the SAM 105<sub>1</sub> can manage access

with respect to the storage region of the external memory 201.

As the external memory 210, use is made of for example a flash memory or a ferro-electric memory (FeRAM).

Also, as the stack memory 200, use is made of for example a SARAM. As shown in Fig. 28, the secure container 104, content key data  $K_c$ , usage control policy data (UCP) 106, a lock key data  $K_{LOC}$  of a storage unit 192, certificate data  $CER_{CP}$  of the content provider 101, usage control status data (UCS) 166, SAM program download containers  $SDC_1$  to  $SDC_3$ , etc. are provided.

Below, among the functions of the SAM 105<sub>1</sub>, the processing contents of the functional blocks when the secure container 104 from the content provider 101 is input will be explained by referring to Fig. 26.

The mutual certification unit 170 performs mutual certification between the content provider 101 and the EMD service center 102 when the SAM 105<sub>1</sub> transmits and receives the data on-line between the content provider 101 and the EMD service center 102 to produce a session key data (common key)  $K_{SES}$  and outputs this to the encryption and/or decryption unit 171. The session key data  $K_{SES}$  is newly produced with each mutual certification.

The encryption and/or decryption unit 171 encrypts and/or decrypts the data transmitted and received between the content provider 101 and the EMD service center 102 by using the session key data  $K_{SES}$  produced by the mutual certification unit 170.

The error correction unit 181 corrects the error of the secure container 104 and outputs the same to the download memory management unit 182.

Note that, it is also possible if the user home network 103 has a function for detecting whether or not the secure container 104 has been tampered with.

In the present embodiment, the case where the error correction unit 181 was built in the SAM 105<sub>1</sub> was exemplified, but it is also possible to impart the function of the error correction unit 181 to the outside of the SAM 105<sub>1</sub>, for example, the host CPU 810.

The download memory management unit 182 performs the mutual certification between the mutual certification unit 170 and a media SAM 167a in a case where the download memory 167 has a media SAM 167a having a mutual certification function as shown in Fig. 25, and then encrypts the secure container 104 after the error correction by using the session key data  $K_{SES}$  obtained by the mutual certification and writes the same into the download memory 167 shown in Fig. 25. As the download



memory 167, use is made of for example a nonvolatile semiconductor memory such as memory stick.

Note that, as shown in Fig. 29, where a memory not provided with a mutual certification function such as a  
5 HDD (hard disk drive) is used as a download memory 211, the inside of the download memory 211 is not secure, so the content file CF is downloaded on the download memory 211, and a key file KF having a high secrecy is downloaded on for example the stack memory 200 shown in  
10 Fig. 26.

The secure container decryption unit 183 decrypts the content key data Kc, usage control policy data 106, and the SAM program download containers SDC<sub>1</sub> to SDC<sub>3</sub> in the key file KF stored in the secure container 104 input  
15 from the download memory management unit 182 by using distribution use key data KD<sub>1</sub> to KD<sub>3</sub> read out from the storage unit 192.

The related decrypted content key data Kc, usage control policy data 106, and the SAM program download  
20 containers SDC<sub>1</sub> to SDC<sub>3</sub> are written into the stack memory 200.

The EMD service center management unit 185 manages the communication with the EMD service center 102 shown in Fig. 1.

25 The signature processing unit 189 verifies the

signature data in the secure container 104 by using a public key data  $K_{ESC,P}$  of the EMD service center 102 read out from the storage unit 192 and the public key data  $K_{CP,P}$  of the content provider 101.

5       The storage unit 192 stores, as the secret data which cannot be read out and rewritten from the outside of the SAM 105<sub>1</sub>, as shown in Fig. 30, a plurality of distribution use key data  $KD_1$  to  $KD_3$  with expiration dates, SAM\_IDs, user IDs, passwords, information  
10   reference use IDs, a SAM registration list, storage use key data  $K_{STR}$ , public key data  $K_{R-CA,P}$  of the route CA, public key data  $K_{ESC,P}$  of the EMD service center 102, media key data  $K_{MED}$ , public key data  $K_{ESC,P}$  of the EMD service center 102, secret key data  $K_{SAM1,S}$  of the SAM 105<sub>1</sub>, the  
15   certificate data  $CER_{SAM1}$  storing public key data  $K_{SAM1,P}$  of the SAM 105<sub>1</sub> therein, signature data  $SIG_{22}$  of the certificate  $CER_{ESC}$  using the secret key data  $K_{ESC,S}$  of the EMD service center 102, the original key data for the mutual certification with the decryption and/or expansion  
20   module 163 (where the common key encryption method is employed), the original key data for the mutual certification with the media SAM (where the common key encryption method is employed), and certificate data  $CER_{MEDSAM}$  of the media SAM (where the public key encryption  
25   method is employed).

Also, in the storage unit 192, a secret program for realizing at least one part of the functions shown in Fig. 26 is stored.

As the storage unit 192, use is made of for example  
5 a flash-EEPROM (electrically erasable programmable RAM).

Below, an explanation will be made of the flow of the processing in the SAM 105<sub>1</sub> when storing the distribution use key data  $KD_1$  to  $KD_3$  received from the EMD service center 102 in the storage unit 192 by  
10 referring to Fig. 26.

In this case, first, mutual certification is carried out between the mutual certification unit 170 and the mutual certification unit 150 shown in Fig. 23.

Next, three months' worth of the distribution use  
15 key data  $K_1$  to  $K_3$  encrypted by the session key data  $K_{SES}$  obtained by the related mutual certification and the signature data  $SIG_{KD1,ESC}$  to  $SIG_{KD3,ESC}$  thereof are written from the EMD service center 102 via the EMD service center management unit 185 into the stack memory 811.

20 Next, in the encryption and/or decryption unit 171, by using the session key data  $K_{SES}$ , the distribution use key data  $K_1$  to  $K_3$  and the signature data  $SIG_{KD1,ESC}$  to  $SIG_{KD3,ESC}$  thereof are decrypted.

Next, in the signature processing unit 189, after  
25 the legitimacy of the signature data  $SIG_{KD1,ESC}$  to  $SIG_{KD3,ESC}$

stored in the stack memory 811 is confirmed, the distribution use key data  $K_1$  to  $K_3$  are written into the storage unit 192.

Below, an explanation will be made of the flow of the processing in the SAM 105<sub>1</sub> receiving as input the secure container 104 provided by the content provider 101 by referring to Fig. 26.

Mutual certification is carried out between the mutual certification unit 170 of the SAM 105<sub>1</sub> shown in Fig. 26 and the mutual certification unit 120 shown in Fig. 3.

The encryption and/or decryption unit 171 decrypts the secure container 104 supplied from the content provider 101 via the content provider management unit 180 by using the session key data  $K_{SES}$  obtained by the related mutual certification.

Next, the signature processing unit 189 verifies the signature data  $SIG_{1,ESC}$  shown in Fig. 5C and then verifies the legitimacy of the signature data  $SIG_{6,CP}$  and  $SIG_{7,CP}$  by using the public key data  $K_{CP,P}$  of the content provider 101 stored in the certificate data  $CER_{CP}$  shown in Fig. 5C.

At this time, when it is verified that the signature data  $SIG_{6,CP}$  is legitimate, the legitimacy of the producer and the transmitter of the content file CF is confirmed.

Also, when it is verified that the signature data  $SIG_{7,CP}$  is legitimate, the legitimacy of the transmitter of the key file KF is confirmed.

Also, the signature processing unit 189 verifies the  
5 legitimacy of the signature data  $SIG_{K1,ESC}$  in the key file  
KF shown in Fig. 5B, that is, the legitimacy of the  
producer of the key file KF and whether or not the key  
file KF is registered in the EMD service center 102 by  
using the public key data  $K_{ESC,P}$  read out from the storage  
10 unit 192.

The content provider management unit 180 outputs the  
secure container 104 to the error correction unit 181  
when the legitimacy of the signature data  $SIG_{6,CP}$ ,  $SIG_{7,CP}$ ,  
and  $SIG_{K1,ESC}$  is confirmed.

15 The error correction unit 181 performs the error  
correction of the secure container 104 and then outputs  
the same to the download memory management unit 182.

The download memory management unit 182 writes the  
secure container 104 into the download memory 167 after  
20 performing the mutual certification between the mutual  
certification unit 170 and the media SAM 167a shown in  
Fig. 25.

Next, the download memory management unit 182  
performs mutual certification between the mutual  
25 certification unit 170 and the media SAM 167a shown in

Fig. 25 and then reads out the key file KF shown in Fig. 5B stored in the secure container 104 from the download memory 167 and outputs the same to the secure container decryption unit 183.

5        Then, in the secure container decryption unit 183, by using the distribution use data  $KD_1$  to  $KD_3$  of the corresponding period input from the storage unit 192, the content key data  $Kc$ , usage control policy data 106, and the SAM program download containers  $SDC_1$  to  $SDC_3$  in the  
10   key file KF shown in Fig. 5B are decrypted.

Then, the decrypted content key data  $Kc$ , usage control policy data 106, and the SAM program download containers  $SDC_1$  to  $SDC_3$  are written into the stack memory 200.

15        Below, an explanation will be made of the processing contents of the functional blocks related to the processing of using and purchasing the content data C downloaded on the download memory 167 by referring to Fig. 31.

20        The usage monitor unit 186 reads out the usage control policy data 106 and the usage control status data 166 from the stack memory 200 and monitors so that the purchase and/or usage of the content is carried out within a range permitted by the related read out usage  
25   control policy data 106 and usage control status data

166.

Here, the usage control policy data 106 is stored in the KF after decryption and stored in the stack memory 200 as explained by using Fig. 26.

5 Also, the usage control status data 166 is stored in the stack memory 200 when the purchase form is determined by the user as will be mentioned later.

The charge processing unit 187 produces the usage log data 108 in response to an operation signal S165 from  
10 the purchase and/or usage form determination operation unit 165 shown in Fig. 25.

Here, the usage log data 108 describes the log of the purchase and usage forms of the secure container 104 by the user as mentioned before and is used when  
15 performing settlement processing in accordance with the purchase of the secure container 104 and determining the payment of the license fee in the EMD service center 102.

Also, the charge processing unit 187 notifies the sales price or the suggested retailer's price data SRP  
20 read out from the stack memory 200 to the user according to need.

Here, the sales price and the suggested retailer's price data SRP have been stored in the usage control policy data 106 of the key file KF shown in Fig. 5B  
25 stored in the stack memory 200 after decryption.

The charge processing by the charge processing unit 187 is carried out based on the right content such as the usage permission condition indicated by the usage control policy data 106 and the usage control status data 166  
5 under the monitoring of the usage monitor unit 186.  
Namely, the user purchases and uses the content within the range according to the related right content, etc.

Also, the charge processing unit 187 produces the usage control status (UCS) data describing the purchase  
10 form of the content by the user and writes this into the stack memory 200.

As the purchase form of the content, there are for example an outright purchase without restriction as to the reproduction by the purchaser and copying for the  
15 usage of the related purchaser, a reproduction charge for charging with each reproduction, etc.

Here, the usage control status data 166 is produced when the user determines the purchase form of the content and is used for control so that the user uses the related  
20 content within the range permitted by the related determined purchase form 5hereafter. In the usage control status data 166, the ID of the content, the purchase form, the price in accordance with the related purchase form, the SAM\_ID of the SAM with the purchase of the  
25 related content performed therefor, the USER\_ID of the



purchased user, etc. are described.

Note that, where the determined purchase form is a reproduction charge, for example, the usage control status data 166 is transmitted from the SAM 105<sub>1</sub> to the content provider 101 in real-time simultaneously with the purchase of the content data C, and the content provider 101 instructs the EMD service center 102 to obtain the usage log data 108 at the SAM 105<sub>1</sub> within the predetermined period.

Also, where the determined purchase form is an outright purchase, for example, the usage control status data 166 is transmitted in real-time to both of the content provider 101 and the EMD service center 102. In this way, in the present embodiment, in both cases, the usage control status data 166 is transmitted in real-time to the content provider 101.

The EMD service center management unit 185 transmits the usage log data 108 read out from the external memory 201 via the external memory management unit 811 to the EMD service center 102.

At this time, the EMD service center management unit 185 produces the signature data  $SIG_{200, SAM1}$  of the usage log data 108 by using the secret key data  $K_{SAM1, S}$  in the signature processing unit 189 and transmits the signature data  $SIG_{200, SAM1}$  together with the usage log data 108 to the

EMD service center 102.

The usage log data 108 can be transmitted to the EMD service center 102 in response to for example a request from the EMD service center 102 or periodically or can be transmitted when the amount of information of the log information contained in the usage log data 108 becomes a predetermined amount or more too. The related amount of information is determined in accordance with for example the storage capacity of the external memory 201.

The download memory management unit 182 outputs the content data C read out from the download memory 167, content key data Kc read out from the stack memory 200, and the user watermark use data 196 input from the charge processing unit 187 to the decryption and/or expansion module management unit 184 in the case where for example a reproduction operation of the content is carried out in response to the operation signal S165 from the purchase form determination operation unit 165 shown in Fig. 25.

Also, the decryption and/or expansion module management unit 184 outputs the content file CF read out from the download memory 167 and the content key data Kc and a half disclosure parameter data 199 read out from the stack memory 200 to the decryption and/or expansion module management unit 184 when a demo operation of the

content is carried out in response to the operation  
signal S165 from the purchase form determination  
operation unit 165 shown in Fig. 25.

Here, the half disclosure parameter data 199 is  
5 described in the usage control policy data 106 and  
indicates the handling of the content in the demo mode.  
In the decryption and/or expansion module 163, it becomes  
possible to reproduce the encrypted content data C in the  
half disclosure state based on the half disclosure  
10 parameter data 199. As the procedure of the half  
disclosure, there is for example a procedure of  
designating the blocks to be decrypted and the blocks not  
to be decrypted by using the content key data Kc,  
limiting the reproduction function at the demo or  
15 limiting a demo enable period by the half disclosure  
parameter data 199 by utilizing the fact that the  
decryption and/or expansion module 163 processes the data  
(signal) in units of predetermined blocks.

Below, an explanation will be made of the flow of  
20 the processing in the SAM 105<sub>1</sub>.

First, an explanation will be made of the flow of  
the processing up to when the purchase form of the secure  
container 104 downloaded on the download memory 167 from  
the content provider 101 is determined by referring to  
25 Fig. 31.

When the operation signal S165 indicating the demo mode is output to the charge processing unit 187 by the operation of the purchase and/or usage form determination operation unit 165 shown in Fig. 25 by the user, for  
5 example, the content file CF stored in the download memory 167 is output via the decryption and/or expansion module management unit 184 to the decryption and/or expansion module 163 shown in Fig. 25.

At this time, for the content file CF, mutual  
10 certification between the mutual certification unit 170 and the media SAM 167a, encryption and/or decryption by the session key data  $K_{SES}$ , mutual certification between the mutual certification unit 170 and the mutual certification unit 220, and encryption and/or decryption  
15 by the session key data  $K_{SES}$  are carried out.

The content file CF is decrypted by using the session key data  $K_{SES}$  at the decryption unit 221 shown in Fig. 25, and then output to the decryption unit 222.

Also, the content key data  $K_c$  and the half  
20 disclosure parameter data 199 read out from the stack memory 200 are output to the decryption and/or expansion module 163 shown in Fig. 25. At this time, after the mutual certification between the mutual certification unit 170 and the mutual certification unit 220,  
25 encryption and decryption by the session key data  $K_{SES}$  are

carried out with respect to the content key data Kc and the half disclosure parameter data 199.

Next, the decrypted half disclosure parameter data 199 is output to the half disclosure processing unit 225.

5 Under the control of the half disclosure processing unit 225, the decryption of the content data C using the content key data Kc by the decryption unit 222 is carried out in half disclosure.

Next, the content data C decrypted in half  
10 disclosure is expanded at the expansion unit 223 and then output to the electronic watermark information processing unit 224.

Next, the user watermark use data 196 is buried in the content data C in the electronic watermark  
15 information processing unit 224, and then the content data C is reproduced at the reproduction module 169, and sound in accordance with the content data C is output.

Then, when the user trying out the content determines the purchase form by operating the purchase  
20 and/or usage form determination operation unit 165, the operation signal S165 indicating the related determined purchase form is output to the charge processing unit 187.

Then, in the charge processing unit 187, the usage  
25 log data 108 and the usage control status data 166 in

accordance with the determined purchase form are produced, the usage log data 108 is written into the external memory 201 via the external memory management unit 811, and, at the same time, the usage control status data 166 is written into the stack memory 200.

Thereafter, in the usage monitor unit 186, control (monitoring) is carried out so that the content data is purchased and used within the range permitted by the usage control status data 166.

Then, a new key file  $KF_1$  shown in Fig. 34C mentioned later is produced, and the related produced key file  $KF_1$  is stored in the download memory 167 via the download memory management unit 182.

As shown in Fig. 34C, the usage control status data 166 stored in the key file  $KF_1$  is sequentially encrypted by using the storage key data  $K_{STR}$  and the media key data  $K_{MED}$  by utilizing the CBC mode of the DES.

Here, the storage use key data  $K_{STR}$  is data determined in accordance with the type of apparatus, for example, a SACD (Super Audio Compact Disc), a DVD (Digital Versatile Disc) apparatus, CD-R apparatus, and MD (Mini Disc) apparatus and is used for establishing one-to-one correspondence between the types of the apparatuses and the types of the storage media. Also, the media key data  $K_{MED}$  is data unique to the storage medium.

Also, in the signature processing unit 189, a hash value  $H_{K1}$  of the key file  $KF_1$  is produced by using the secret key data  $K_{SAM1,S}$  of the SAM 105<sub>1</sub>, and the related produced hash value  $H_{K1}$  is written into the stack memory 200 in correspondence to the key file  $KF_1$ . The hash value  $H_{K1}$  is used for verifying the legitimacy of the producer of the key file  $KF_1$  and whether or not the key file  $KF_1$  was tampered with.

Next, the flow of the processing where the content data C with the purchase form already determined therefor stored in the download memory 167 will be explained by referring to Fig. 31.

In this case, under the monitoring of the usage monitor unit 186, based on the operation signal S165, the content file CF stored in the download memory 167 is output to the decryption and/or expansion module 163 shown in Fig. 31. At this time, mutual certification is carried out between the mutual certification unit 170 shown in Fig. 31 and the mutual certification unit 220 of the decryption and/or expansion module 163 shown in Fig. 25.

Also, the content key data  $Kc$  read out from the stack memory 200 is output to the decryption and/or expansion module 163.

Then, in the decryption unit 222 of the decryption

and/or expansion module 163, the decryption of the content file CF using the content key data Kc and the expansion processing by an expansion unit 223 are carried out, and in the reproduction module 169, the content data  
5 C is reproduced.

At this time, by the charge processing unit 187, the usage log data 108 stored in the external memory 201 is updated in accordance with the operation signal S165.

The usage log data 108 is read out from the external  
10 memory 201, and then, after passing through the mutual certification, transmitted via the EMD service center management unit 185 together with the signature data SIG<sub>200, SAM1</sub> to the EMD service center 102.

Next, as shown in Fig. 32, the flow of the  
15 processing in the SAM 105<sub>1</sub> in a case where for example, after the purchase form of the content file CF downloaded on the download memory 167 of the network apparatus 160<sub>1</sub> is determined as mentioned above, a new secure container 104x storing the related content file CF is produced, and  
20 the secure container 104x is transferred via the bus 191 to the SAM 105<sub>2</sub> of the AV apparatus 160<sub>2</sub> will be explained by referring to Fig. 33.

The user operates the purchase and/or usage form determination operation unit 165 and instructs the  
25 transfer of the predetermined content stored in the



download memory 167 to the AV apparatus 160<sub>2</sub>, and the operation signal S165 in accordance with the related operation is output to the charge processing unit 187.

By this, the charge processing unit 187 updates the  
5 usage log data 108 stored in the external memory 201 based on the operation signal S165.

Also, the charge processing unit 187 transmits the usage control status data 166 indicating the related determined purchase form via the EMD service center  
10 management unit 185 to the EMD service center 102 whenever the purchase form of the content data is determined.

Also, the download memory management unit 182 outputs the content file CF and the signature data SIG<sub>6,CP</sub>  
15 thereof shown in Fig. 5A, the key file KF and the signature data SIG<sub>7,CP</sub> thereof, and the key file KF<sub>1</sub> and the hash value H<sub>K1</sub> thereof read out from the download memory 167 to the SAM management unit 190. At this time, the mutual certification between the mutual certification  
20 unit 170 of the SAM 105<sub>1</sub> and the media SAM 167a and the encryption and/or decryption by the session key data K<sub>SES</sub> are carried out.

Also, the signature processing unit 189 obtains the hash value of the content file CF, produces signature  
25 data SIG<sub>41,SAM1</sub> by using the secret key data K<sub>SAM1,S</sub>, and

outputs this to the SAM management unit 190.

Also, the signature processing unit 189 obtains the hash value of the key file  $KF_1$ , produces signature data  $SIG_{42, SAM1}$  by using the secret key data  $K_{SAM1, S}$ , and outputs  
5 this to the SAM management unit 190.

Also, the SAM management unit 190 reads out the certificate data  $CER_{CP}$  and the signature data  $SIG_{1, ESC}$  thereof and the certificate data  $CER_{SAM1}$  and the signature data  $SIG_{22, ESC}$  thereof shown in Fig. 34D from the storage  
10 unit 192.

Also, the mutual certification unit 170 outputs the session key data  $K_{SES}$  obtained by performing the mutual certification with the SAM 105<sub>2</sub> to the encryption and/or decryption unit 171.

15 The SAM management unit 190 produces a new secure container 104x comprised of the data shown in Figs. 34A, 34B, 34C, and 34D, encrypts the secure container 104x in the encryption and/or decryption unit 171 by using the session key data  $K_{SES}$ , and then outputs the same to the  
20 SAM 105<sub>2</sub> of the AV apparatus 160<sub>2</sub> shown in Fig. 32.

At this time, in parallel to the mutual certification between the SAM 105<sub>1</sub> and the SAM 105<sub>2</sub>, mutual certification of the bus 191 serving as the IEEE1394 serial bus is carried out.

25 Below, as shown in Fig. 32, the flow of the

processing in the SAM 105<sub>2</sub> when writing the secure container 104x input from the SAM 105<sub>1</sub> into the storage medium 130<sub>4</sub> of a RAM type or the like will be explained by referring to Fig. 35.

5        Here, the RAM type storage medium 130<sub>4</sub> has for example an unsecure RAM region 134, a media SAM 133, and a secure RAM region 132.

10        In this case, the SAM management unit 190 of the SAM 105<sub>2</sub> receives as input the secure container 104x from the SAM 105<sub>1</sub> of the network apparatus 160<sub>1</sub> as shown in Fig. 32 and Fig. 35.

15        Then, in the encryption and/or decryption unit 171, the secure container 104x input via the SAM management unit 190 is decrypted by using the session key data  $K_{SES}$  obtained by the mutual certification between the mutual certification unit 170 and the mutual certification unit 170 of the SAM 105<sub>1</sub>.

20        Next, in the signature processing unit 189, the legitimacy of the signature data  $SIG_{6,CP}$  is verified by using the public key data  $K_{CP,P}$ , and the legitimacy of the producer of the content file CF is confirmed. Also, in the signature processing unit 189, the legitimacy of the signature data  $SIG_{41,SAM1}$  is verified by using the public key data  $K_{SAM1,P}$ , and the legitimacy of the transmitter of  
25        the content file CF is confirmed.

Then, after it is confirmed that the producer and the transmitter of the content file CF are legitimate, the content file CF is output from the SAM management unit 190 to a storage module management unit 855, and the content file CF is written into the RAM region 134 of the RAM type storage medium 130<sub>4</sub> shown in Fig. 32.

Also, the key file KF and the signature data SIG<sub>7,CP</sub> and SIG<sub>42,SAM1</sub> thereof, the key file KF<sub>1</sub> and the hash value K<sub>K1</sub> thereof, the certificate data CER<sub>CP</sub> and the signature data SIG<sub>1,ESC</sub> thereof, and the certificate data CER<sub>SAM1</sub> and the signature data SIG<sub>22,ESC</sub> thereof decrypted by using the session key data K<sub>SES</sub> are written into the stack memory 200.

Next, the signature processing unit 189 verifies the signature data SIG<sub>22,ESC</sub> read out from the stack memory 200 by using the public key data K<sub>ESC,P</sub> read out from the storage unit 192 and confirms the legitimacy of the certificate data CER<sub>SAM1</sub>.

Then, the signature processing unit 189 verifies the legitimacy of the signature data SIG<sub>42,SAM1</sub> stored in the stack memory 200 by using the public key data K<sub>SAM1,P</sub> stored in the certificate data CER<sub>SAM1</sub> when confirming the legitimacy of the certificate data CER<sub>SAM1</sub>. Then, when it is verified that the signature data SIG<sub>42,SAM1</sub> is legitimate, the legitimacy of the key file KF is

confirmed.

Also, the signature processing unit 189 verifies the signature data  $SIG_{1,ESC}$  read out from the stack memory 200 by using the public key data  $K_{ESC,P}$  read out from the storage unit 192 and confirms the legitimacy of the certificate data  $CER_{CP}$ .

Then, the signature processing unit 189 verifies the legitimacy of the signature data  $SIG_{7,SAM1}$  stored in the stack memory 200 by using the public key data  $K_{CP,P}$  stored in the certificate data  $CER_{CP}$  when confirming the legitimacy of the certificate data  $CER_{CP}$ . Then, when it is verified that the signature data  $SIG_{7,SAM1}$  is legitimate, the legitimacy of the producer of the key file KF is confirmed.

When it is confirmed that the producer and the transmitter of the key file KF are legitimate, the key file KF is read out from the stack memory 200 and written into the secure RAM region 132 of the RAM type storage medium 130<sub>4</sub> shown in Fig. 34 via the storage module management unit 855.

Also, the signature processing unit 189 verifies the legitimacy of the hash value  $H_{K1}$  by using the public key data  $K_{SAM1,P}$  and confirms the legitimacy of the producer and transmitter of the key file  $KF_1$ .

Then, when the legitimacy of the producer and the

transmitter of the key file  $KF_1$  is confirmed, the key file  $KF_1$  shown in Fig. 34C is read out from the stack memory 200 and output to the encryption and/or decryption unit 173.

5        Note that, in the related example, the case where the producer and the transmitter of the key file  $KF_1$  were the same was mentioned, but where the producer and the transmitter of the key file  $KF_1$  are different, the signature data of the producer and the signature data of the transmitter are produced with respect to the key file  $KF_1$ , and the legitimacy of the both signature data is verified in the signature processing unit 189.

Then, the encryption and/or decryption unit 173 encrypts the content key data  $K_c$  and the usage control status data 166 in the key file  $KF_1$  by sequentially using the storage use key data  $K_{STR}$ , media key data  $K_{MED}$ , and the purchaser key data  $K_{PIN}$  read out from the storage unit 192 and outputs the same to the storage module management unit 855.

20        Then, by the storage module management unit 855, the encrypted key file  $KF_1$  is stored in the secure RAM region 132 of the RAM type storage medium 130<sub>4</sub>.

Note that, the media key data  $K_{MED}$  is stored in the storage unit 192 in advance by the mutual certification between the mutual certification unit 170 shown in Fig.

25

33 and the media SAM 133 of the RAM type storage medium 130<sub>4</sub> shown in Fig. 32.

Here, the storage use key data  $K_{STR}$  is data determined in accordance with the type of apparatus (AV apparatus 160<sub>2</sub> in the related example) of for example the SACD (Super Audio Compact Disc), DVD (Digital Versatile Disc) apparatus, CD-R apparatus, and MD (Mini Disc) apparatus and is used for establishing one-to-one correspondence between the types of the apparatuses and the types of the storage media. Note that, the physical structures of the disc media are the same between SACD and DVD, so there is a case where the recording and/or reproduction of the storage medium of an SACD can be carried out by using a DVD apparatus. The storage use key data  $K_{STR}$  performs the function of preventing illegitimate copies in such a case.

Note that, in the present embodiment, it is also possible not to encrypt using the storage use key data  $K_{STR}$ .

Also, the media key data  $K_{MED}$  is data unique to the storage medium (RAM type storage medium 130<sub>4</sub> in the related example).

The media key data  $K_{MED}$  is stored in the storage medium (RAM type storage medium 130<sub>4</sub> shown in Fig. 32 in the related example). It is preferred from the viewpoint

of the security that encryption and the decryption using the media key data  $K_{MED}$  be carried out in the media SAM of the storage medium. At this time, the media key data  $K_{MED}$  is stored in the related media SAM where the media SAM is mounted in the storage medium, while is stored in for example a region out of management of the host CPU 810 in the RAM region where the media SAM is not mounted in the storage medium.

Note that, it is also possible to perform the mutual certification between the apparatus side SAM (SAM 105<sub>2</sub> in the related example) and the media SAM (media SAM 133 in the related example), transfer the media key data  $K_{MED}$  via the secure communication route to the apparatus side SAM, and perform the encryption and decryption using the media key data  $K_{MED}$  in the apparatus side SAM as in the present embodiment.

In the present embodiment, the storage use key data  $K_{STR}$  and the media key data  $K_{MED}$  are used for protecting the security of the level of the physical layer of the storage medium.

Also, the purchaser key data  $K_{PIN}$  is data indicating the purchaser of the content file CF and is allocated by the EMD service center 102 to the related purchased user when for example the content is purchased by outright purchase. The purchaser key data  $K_{PIN}$  is managed in the



EMD service center 102.

Also, in the above embodiment, the case where the key files KF and KF<sub>1</sub> were stored in the secure RAM region 132 of the RAM type storage medium 130<sub>4</sub> by using the storage module 260 was exemplified, but as indicated by a dotted line in Fig. 32, it is also possible to store the key files KF and KF<sub>1</sub> in the media SAM 133 from the SAM 105<sub>2</sub>.

Next, the flow of the processing when determining the purchase form in the AV apparatus 160<sub>2</sub> where the user home network 303 is distributed the ROM type storage medium 130<sub>1</sub> shown in Fig. 12 with the purchase form of the content undetermined therefor off-line will be explained by referring to Fig. 36 and Fig. 37.

The SAM 105<sub>2</sub> of the AV apparatus 160<sub>2</sub> first performs the mutual certification between the mutual certification unit 170 shown in Fig. 37 and the media SAM 133 of the ROM type storage medium 130<sub>1</sub> shown in Fig. 12, and then receives as input the media key data K<sub>MED</sub> from the media SAM 133.

Note that, where the SAM 105<sub>2</sub> holds the media key data K<sub>MED</sub> in advance, it is also possible if the related input is not carried out.

Next, the key file KF and the signature data SIG<sub>7,CP</sub> thereof and the certificate data CER<sub>CP</sub> and the signature

data  $SIG_{1,ESC}$  thereof shown in Figs. 5B and 5C stored in the secure container 104 stored in the secure RAM region 132 of the ROM type storage medium 130<sub>1</sub> are input via the media SAM management unit 197 or not illustrated read out module management unit and are written into the stack memory 200.

Next, in the signature processing unit 189, after the legitimacy of the signature data  $SIG_{1,ESC}$  is confirmed, the public key data  $K_{CP,P}$  is extracted from the certificate data  $CER_{CP}$ , and by using this public key data  $K_{CP,P}$ , the legitimacy of the signature data  $SIG_{7,CP}$ , that is, the legitimacy of the transmitter of the key file KF is verified.

Also, in the signature processing unit 189, by using the public key data  $K_{ESC,P}$  read out from the storage unit 192, the legitimacy of the signature data  $SIG_{K1,ESC}$  stored in the key file KF, that is, the legitimacy of the producer of the key file KF, is verified.

When the legitimacy of the signature data  $SIG_{7,CP}$  and  $SIG_{K1,ESC}$  is confirmed in the signature processing unit 189, the key file KF is read out from the stack memory 200 to the secure container decryption unit 183.

Next, in the secure container decryption unit 183, by using the distribution use data  $KD_1$  to  $KD_3$  of the corresponding period, the content key data  $Kc$ , usage

control policy data 106, and the SAM program download containers  $SDC_1$  to  $SDC_3$  stored in the key file KF are decrypted and are written into the stack memory 200.

Next, after the mutual certification between the  
5 mutual certification unit 170 shown in Fig. 37 and the decryption and/or expansion module 163 shown in Fig. 36, the decryption and/or expansion module management unit 184 of the SAM 105<sub>2</sub> outputs the content key data Kc stored in the stack memory 200 and the half disclosure  
10 parameter data 199 stored in the usage control policy data 106 and the content data C stored in the content file CF read out from the ROM region 131 of the ROM type storage medium 130<sub>1</sub> to the decryption and/or expansion module 163 shown in Fig. 36. Next, in the decryption  
15 and/or expansion module 163, the content data C is decrypted in the half disclosure mode by using the content key data Kc and then expanded and output to a reproduction module 270. Then, in the reproduction module 270, the content data C from the decryption and/or  
20 expansion module 163 is reproduced.

Next, the purchase form of the content is determined by the purchase operation of the purchase form determination operation unit 165 shown in Fig. 36 by the user, and the operation signal S165 indicating the  
25 related determined purchase form is input to the charge

processing unit 187.

Next, the charge processing unit 187 produces the usage control status data 166 in response to the operation signal S165 and writes this into the stack

5 memory 200.

Next, the content key data Kc and the usage control status data 166 are output from the stack memory 200 to the encryption and/or decryption unit 173.

Next, the encryption and/or decryption unit 173  
10 sequentially encrypts the content key data Kc and the usage control status data 166 input from the stack memory 200 by using the storage use key data  $K_{STR}$ , the media key data  $K_{MED}$ , and the purchaser key data  $K_{PIN}$  read out from the storage unit 192 and writes them into the stack  
15 memory 200.

Next, in the media SAM management unit 197, the key file  $KF_1$  shown in Fig. 34C is produced by using the encrypted content key data Kc, the usage control status data 166 and the SAM program download containers  $SDC_1$  to  
20  $SDC_3$  read out from the stack memory 200.

Also, in the signature processing unit 189, the hash value  $H_{K1}$  of the key file  $KF_1$  shown in Fig. Figure C is produced, and the related hash value  $H_{K1}$  is output to the media SAM management unit 197.

25 Next, after the mutual certification between the

mutual certification unit 170 shown in Fig. 37 and the media SAM 133 shown in Fig. 36, the media SAM management unit 197 writes the key file  $KF_1$  and the hash value  $H_{K1}$  into the secure RAM region 132 of the ROM type storage medium 130<sub>1</sub> via a storage module 271 shown in Fig. 36.

By this, the ROM type storage medium 130<sub>1</sub> with the purchase form determined therefor is obtained.

At this time, the usage control status data 166 and the usage log data 108 produced by the charge processing unit 187 are read out from the stack memory 200 and the external memory 201 at the predetermined timing and transmitted to the EMD service center 102.

Note that, where the key file  $KF$  is stored in the media SAM 133 of the ROM type storage medium 130<sub>1</sub>, as indicated by the dotted line in Fig. 36, the SAM 105<sub>2</sub> receives as input the key file  $KF$  from the media SAM 133. Also, in this case, the SAM 105<sub>2</sub> writes the produced key file  $KF_1$  into the media SAM 133.

Below, as shown in Fig. 38, the flow of the processing when the secure container 104 is read out from the ROM type storage medium 130<sub>1</sub> with the purchase form undetermined therefor in the AV apparatus 160<sub>3</sub> to produce a new secure container 104<sub>y</sub>, this is transferred to the AV apparatus 160<sub>2</sub>, the purchase form is determined in the AV apparatus 160<sub>2</sub>, and this is written into a RAM type

storage medium 130<sub>5</sub> will be explained by referring to Fig. 39 and Fig. 40.

Note that, the transfer of the secure container 104 from the ROM type storage medium 130<sub>1</sub> to the RAM type storage medium 130<sub>5</sub> can be carried out between the network apparatus 160<sub>1</sub> shown in Fig. 1 and any of the AV apparatuses 160<sub>1</sub> to 160<sub>4</sub> shown in Fig. 1.

First, mutual certification is carried out between the SAM 105<sub>3</sub> of the AV apparatus 160<sub>3</sub> and the media SAM 133 of the ROM type storage medium 130<sub>1</sub>, and media key data  $K_{MED1}$  of the ROM type storage medium 130<sub>1</sub> is transferred to the SAM 105<sub>3</sub>.

Also, mutual certification is carried out between the SAM 105<sub>2</sub> of the AV apparatus 160<sub>2</sub> and the media SAM 133 of the RAM type storage medium 130<sub>5</sub>, and media key data  $K_{MED2}$  of the RAM type storage medium 130<sub>5</sub> is transferred to the SAM 105<sub>2</sub>.

Note that, where encryption using the media key data  $K_{MED1}$  and  $K_{MED2}$  is carried out in the media SAM 133 and the media SAM 133, the transfer of the media key data  $K_{MED1}$  and  $K_{MED2}$  is not carried out.

Next, the SAM 105<sub>3</sub> outputs the content file CF and the signature data  $SIG_{6,CP}$  thereof shown in Fig. 5A read out from the ROM region 131 of the ROM type storage medium 130<sub>1</sub>, the key file KF and the signature data  $SIG_{7,CP}$

thereof shown in Figs. 5B and 5C read out from the secure RAM region 132, and the certificate data  $CER_{CP}$  and the signature data  $SIG_{1,ESC}$  thereof to the encryption and/or decryption unit 171 via the media SAM management unit 197

5 or not illustrated read out module management unit as shown in Fig. 39.

Also, the content file CF and the key file KF are output from the media SAM management unit 197 to the signature processing unit 189.

10 Then, in the signature processing unit 189, the hash values of the content file CF and the key file KF are obtained, signature data  $SIG_{350,SAM3}$  and  $SIG_{352,SAM3}$  are produced by using secret key data  $K_{SAM3,s}$ , and they are output to the encryption and/or decryption unit 171.

15 Also, the certificate data  $CER_{SAM3}$  and the signature data  $SIG_{351,ESC}$  thereof are read out from the storage unit 192 and output to the encryption and/or decryption unit 171.

Then, the secure container 104y shown in Fig. 40 is  
20 encrypted by using the session key data  $K_{SES}$  obtained by mutual certification between the SAM 105<sub>3</sub> and 105<sub>2</sub> in the encryption and/or decryption unit 171 and then output via the SAM management unit 190 to the SAM 105<sub>2</sub> of the AV apparatus 160<sub>1</sub>.

25 In the SAM 105<sub>2</sub>, as shown in Fig. 41, the secure

container 104y shown in Fig. 40 input from the SAM 105<sub>3</sub>,  
via the SAM management unit 190 is decrypted in the  
encryption and/or decryption unit 171 by using the  
session key data  $K_{SES}$ , and then the legitimacy of the  
5 signature data  $SIG_{6,CP}$  and  $SIG_{350,SAM3}$  stored in the secure  
container 104y, that is, the legitimacy of the producer  
and the transmitter of the content file CF is confirmed.

Then, after it is confirmed that the producer and  
the transmitter of the content file CF are legitimate,  
10 the content file CF is written into the RAM region 134 of  
the RAM type storage medium 130<sub>5</sub> via the media SAM  
management unit 197.

Also, after the key file KF and the signature data  
 $SIG_{7,CP}$  and  $SIG_{350,SAM3}$  thereof and certificate data  $CER_{SAM3}$   
15 and the signature data  $SIG_{351,ESC}$  thereof input from the  
SAM 105<sub>3</sub> via the SAM management unit 190 are written into  
the stack memory 200, they are decrypted in the  
encryption and/or decryption unit 171 by using the  
session key data  $K_{SES}$ .

20 Next, the related decrypted signature data  $SIG_{351,ESC}$   
is verified in the signature processing unit 189. When  
the legitimacy of the certificate data  $CER_{SAM3}$  is  
confirmed, by using the public key data  $K_{SAM3}$  stored in  
the certificate data  $CER_{SAM3}$ , the legitimacy of the  
25 signature data  $SIG_{7,CP}$  and  $SIG_{352,SAM3}$ , that is, the



legitimacy of the producer and the transmitter of the key file KF is confirmed.

Then, when the legitimacy of the producer and the transmitter of the key file KF is confirmed, the key file  
5 KF is read out from the stack memory 200 and output to the secure container decryption unit 183.

Next, the secure container decryption unit 183 decrypts the key file KF by using the distribution use data  $KD_1$  to  $KD_3$  of the corresponding period and writes  
10 the related decrypted key file KF into the stack memory 200.

Next, the usage control policy data 106 stored in the already decrypted key file KF stored in the stack memory 200 is output to the usage monitor unit 186. The  
15 usage monitor unit 186 manages the purchase form and usage form of the content based on the usage control policy data 106.

Next, for example, when the demo mode is selected by the user, the content data C of the content file CF  
20 already decrypted by the session key data  $K_{SES}$ , the content key data  $K_c$  stored in the stack memory 200, the half disclosure parameter data 199 obtained from the usage control policy data 106, and the user watermark use data 196 are output via the decryption and/or expansion  
25 module management unit 184 shown in Fig. 38 to the

reproduction module 270 after passing through mutual certification. Then, in the reproduction module 270, the reproduction of the content data C corresponding to the demo mode is carried out.

5       Next, the purchase and/or usage form of the content is determined by the operation of the purchase and/or usage form determination operation unit 165 shown in Fig. 38 by the user, and the operation signal S165 in accordance with the related determination is output to  
10      the charge processing unit 187.

Then, in the charge processing unit 187, the usage control status data 166 and the usage log data 108 are produced in accordance with the determined purchase and/or usage form and are written into the stack memory  
15      200 and the external memory 201.

Next, the content key data Kc and the usage control status data 166 are read out from the stack memory 200 to the encryption and/or decryption unit 173, sequentially encrypted in the encryption and/or decryption unit 173 by  
20      using the storage use key data  $K_{STR}$ , media key data  $K_{MED2}$ , and the purchaser key data  $K_{PIN}$  read out from the storage unit 192, and output to the storage module management unit 855. Then, for example, in the storage module management unit 855, the key file  $KF_1$  shown in Fig. 34C  
25      is produced, and the key file  $KF_1$  is written into the

media SAM 133 of the RAM type storage medium 130<sub>5</sub> via the media SAM management unit 197.

Also, the content file CF stored in the secure container 104y is written into the RAM region 134 of the RAM type storage medium 130<sub>5</sub> by the storage module management unit 855.

Also, the usage control status data 166 and the usage log data 108 are transmitted to the EMD service center 102 at the predetermined timing.

Below, an explanation will be made of the method of realization of the SAMs 105<sub>1</sub> to 105<sub>4</sub>.

Where the functions of the SAMs 105<sub>1</sub> to 105<sub>4</sub> are realized as hardware, by using an ASIC type CPU including a memory, data having a high degree of secrecy such as a security functional module for realizing the functions shown in Fig. 26, program module for performing the rights clearing of the content, and the key data are stored in that memory. One series of rights clearing use program modules such as an encryption library module (public key code, common key code, random number generator, hash function), program module for the usage control of the content, and the program module of the charge processing are mounted as for example software.

For example, a module such as the encryption and/or decryption unit 171 shown in Fig. 26 is mounted as an IP

core in the ASIC type CPU as hardware due to the problem  
of for example processing speed. Depending on the clock  
speed or performance of the CPU code system etc., it is  
also possible to mount the encryption and/or decryption  
5 unit 171 as software.

Also, as the storage unit 192 shown in Fig. 26, the  
program module for realizing the functions shown in Fig.  
26, and the memory for storing the data, use is made of  
for example a nonvolatile memory (flash-ROM), while as  
10 the working memory, a high speed writable memory such as  
an SRAM is used. Note that, other than them, as the  
memory included in the SAMs 105<sub>1</sub> to 105<sub>4</sub>, it is also  
possible to use a ferroelectric memory (FeRAM).

Also, in the SAMs 105<sub>1</sub> to 105<sub>4</sub>, other than the  
15 above, a clock function used for the verification of the  
date in the expiration date and the contract period etc.  
for the usage of the content is included.

As mentioned above, the SAMs 105<sub>1</sub> to 105<sub>4</sub> have  
tamper resistance sheltering the program module, data,  
20 and the processing content from the outside. In order to  
prevent the program and content of data having high  
secrecy stored in the memory inside the IC of the related  
SAM and values of the register group related to the  
system configuration of the SAM and the encryption  
25 library and the register group of the clock from being

read out and newly written via the bus of the host CPU of  
the apparatuses with the SAMs 105<sub>1</sub> to 105<sub>4</sub> mounted  
thereon, that is, in order to prevent the host CPU of the  
mounted apparatus from not existing in the allocated  
5 address space, an address space not seen from the host  
CPU on the mounted apparatus side is set up in the  
related SAM by using an MMU (memory management unit) for  
managing the memory space on the CPU side.

Also, the SAMs 105<sub>1</sub> to 105<sub>4</sub> have structures durable  
10 against physical attack from the outside such as X-rays  
or heat and further have structures such that, even if  
real-time debugging (reverse engineering) using a debug  
use tool (hardware ICE or software ICE) or the like is  
carried out, the processing content thereof cannot be  
15 seen or the debug use tool per se cannot be used after  
the manufacture of the IC.

The SAMs 105<sub>1</sub> to 105<sub>4</sub> per se are usual ASIC type  
CPUs including memories in the hardware structure. Their  
functions depend on the software for operating the  
20 related CPU, but are different from the general ASIC type  
CPU in the point that they have a hardware structure of  
the encryption function and tamper resistance.

Where all of the functions of the SAMs 105<sub>1</sub> to 105<sub>4</sub>  
are realized by software, there are cases where the  
25 software processing is carried out by enclosing the same

inside a module having the tamper resistance and cases where they are achieved by software processing on the host CPU mounted on the usual set and steps are taken so that decipherment becomes impossible at only the related processing. The former is the same as the case where an encryption library module is stored in the memory as not the IP core, but the usual software module, and can be considered similar to the case where the functions are realized as the hardware. On the other hand, the latter is referred to as tamper resistant software. Even if the execution situation is deciphered by the ICE (debugger), the execution sequence of the tasks is scattered (in this case, tasks are divided so that the a divided task has a meaning as a program, that is, no influence will be exerted upon the lines before and after that), and the tasks per se are encrypted, so one type of secure processing can be realized similar to a task scheduler (MiniOS). The related task scheduler is buried in the target program.

Next, an explanation will be made of the decryption and/or expansion module 163 shown in Fig. 25.

As shown in Fig. 25, the decryption and/or expansion module 163 has the mutual certification unit 220, decryption unit 221, decryption unit 222, expansion unit 223, electronic watermark information processing unit

224, and the half disclosure processing unit 225.

The mutual certification unit 220 performs the mutual certification with the mutual certification unit 170 shown in Fig. 32 when the decryption and/or expansion module 163 receives as its input the data from the SAM 105<sub>1</sub> and produces the session key data  $K_{SES}$ .

The decryption unit 221 decrypts the content key data  $K_c$ , half disclosure parameter data 199, user watermark use data 196, and the content data C input from the SAM 105<sub>1</sub> by using the session key data  $K_{SES}$ . Then, the decryption unit 221 outputs the decrypted content key data  $K_c$  and the content data C to the decryption unit 222, outputs the decrypted user watermark use data 196 to the electronic watermark information processing unit 224, and outputs the half disclosure parameter data 199 to the half disclosure processing unit 225.

The decryption unit 222 decrypts the content data C in the half disclosure mode by using the content key data  $K_c$  under the control from the half disclosure processing unit 225 and outputs the decrypted content data C to the expansion unit 223.

The expansion unit 223 expands the decrypted content data C and outputs the same to the electronic watermark information processing unit 224.

The expansion unit 223 performs the expansion

processing by using the A/V expansion use software stored in the content file CF shown in Fig. 5A and performs the expansion processing by for example the ATRAC3 method.

The electronic watermark information processing unit 5 224 buries the user watermark in accordance with decrypted user watermark use data 196 in the decrypted content data C and produces new content data C. The electronic watermark information processing unit 224 outputs the related new content data C to the 10 reproduction module 169.

In this way, the user watermark is buried at the decryption and/or expansion module 163 when reproducing the content data C.

Note that, in the present invention, it is also 15 possible if the user watermark use data 196 is not buried in the content data C.

The half disclosure processing unit 225 instructs the blocks not to be decrypted and the blocks to be decrypted in for example the content data C to the 20 decryption unit 222 based on the half disclosure parameter data 199.

Also, the half disclosure processing unit 225 performs the control such as limiting the reproduction function at the time of a demo or the demo period based 25 on the half disclosure parameter data 199.



The reproduction module 169 performs the reproduction in accordance with the decrypted and expanded content data C,

Next, an explanation will be made of the data format  
5 when transmitting and receiving data with the signature data produced by using the secret key data attached thereto and the certificate data among the content provider 101, EMD service center 102, and the user home network 103.

10 Figure 42A is a view for explaining the data format where the data Data is transmitted from the content provider 101 to the SAM 105<sub>1</sub> by the in-band method.

In this case, a module Mod<sub>50</sub> encrypted by the session key data K<sub>SES</sub> obtained by the mutual certification  
15 between the content provider 101 and the SAM 105<sub>1</sub> is transmitted from the content provider 101 to the SAM 105<sub>1</sub>.

In the module Mod<sub>50</sub>, a module Mod<sub>51</sub> and the signature data SIG<sub>CP</sub> by the secret key data K<sub>CP,S</sub> thereof are stored.

20 In the module Mod<sub>51</sub>, the certificate data CER<sub>CP</sub> storing the secret key data K<sub>CP,P</sub> of the content provider 101, the signature data SIG<sub>ESC</sub> based on the secret key data K<sub>ESC,S</sub> with respect to the certificate data CER<sub>CP</sub>, and the data Data to be transmitted are stored.

25 In this way, by transmitting the module Mod<sub>50</sub>

storing the certificate data  $CER_{CP}$  from the content provider 101 to the SAM 105<sub>1</sub>, when verifying the signature data  $SIG_{CP}$  at the SAM 105<sub>1</sub>, it becomes unnecessary to transmit the certificate data  $CER_{CP}$  from  
5 the EMD service center 102 to the SAM 105<sub>1</sub>.

Figures 42B and 42C are views for explaining the data format where the data Data is transmitted from the content provider 101 to the SAM 105<sub>1</sub> by the out-of-band method.

10 In this case, a module  $Mod_{52}$  shown in Fig. 42B encrypted by the session key data  $K_{SES}$  obtained by the mutual certification between the content provider 101 and the SAM 105<sub>1</sub> is transmitted from the content provider 101 to the SAM 105<sub>1</sub>.

15 In the module  $Mod_{52}$ , the data Data to be transmitted and the signature data  $SIG_{CP}$  by the secret key data  $K_{CP,S}$  thereof are stored.

Further, a module  $Mod_{53}$  shown in Fig. 42C encrypted by the session key data  $K_{SES}$  obtained by the mutual  
20 certification between the EMD service center 102 and the SAM 105<sub>1</sub> is transmitted from the EMD service center 102 to the SAM 105<sub>1</sub>.

In the module  $Mod_{53}$ , the certificate data  $CER_{CP}$  of the content provider 101 and the signature data  $SIG_{ESC}$  by  
25 the secret key data  $K_{ESC,S}$  thereof are stored.

Figure 42D is a view for explaining the data format of the case where the data Data is transmitted from the SAM 105<sub>1</sub> to the content provider 101 by the in-band method.

5        In this case, a module Mod<sub>54</sub> encrypted by the session key data K<sub>SES</sub> obtained by the mutual certification between the content provider 101 and the SAM 105<sub>1</sub> is transmitted from the SAM 105<sub>1</sub> to the content provider 101.

10       In the module Mod<sub>54</sub>, a module Mod<sub>55</sub> and the signature data SIG<sub>SAM1</sub> by the secret key data K<sub>SAM1,S</sub> thereof are stored.

15       In the module Mod<sub>55</sub>, the certificate data CER<sub>SAM1</sub> storing the secret key data K<sub>SAM1,P</sub> of the SAM 105<sub>1</sub>, the signature data SIG<sub>ESC</sub> by the secret key data K<sub>ESC,S</sub> with respect to the certificate data CER<sub>SAM1</sub>, and the data Data to be transmitted are stored.

20       In this way, by transmitting the module Mod<sub>55</sub> storing the certificate data CER<sub>SAM1</sub> from the SAM 105<sub>1</sub> to the content provider 101, when verifying the signature data SIG<sub>SAM1</sub> in the content provider 101, it becomes unnecessary to transmit the certificate data CER<sub>SAM1</sub> from the EMD service center 102 to the content provider 101.

25       Figures 42E and 42F are views for explaining the data format where the data Data is transmitted from the

SAM 105<sub>1</sub> to the content provider 101 by the out-of-band method.

In this case, a module Mod<sub>56</sub> shown in Fig. 42E encrypted by the session key data K<sub>SES</sub> obtained by the mutual certification between the content provider 101 and the SAM 105<sub>1</sub> is transmitted from the SAM 105<sub>1</sub> to the content provider 101.

In the module Mod<sub>56</sub>, the data Data to be transmitted and the signature data SIG<sub>SAM1</sub> by the secret key data K<sub>SAM1,S</sub> thereof are stored.

Also, from the EMD service center 102 to the content provider 101, a module Mod<sub>57</sub> shown in Fig. 42F encrypted by session key data K<sub>SES</sub> obtained by the mutual certification between the EMD service center 102 and the content provider 101 is transmitted.

In the module Mod<sub>57</sub>, the certificate data CER<sub>SAM1</sub> of the SAM 105<sub>1</sub> and the signature data SIG<sub>ESC</sub> by the secret key data K<sub>ESC,S</sub> thereof are stored.

Figure 43G is a view for explaining the data format where the data Data is transmitted from the content provider 101 to the EMD service center 102 by the in-band method.

In this case, a module Mod<sub>58</sub> encrypted by the session key data K<sub>SES</sub> obtained by the mutual certification between the content provider 101 and the EMD service

center 102 is transmitted from the content provider 101 to the EMD service center 102.

In the module  $Mod_{58}$ , a module  $Mod_{59}$  and the signature data  $SIG_{CP}$  by the secret key data  $K_{CP,S}$  thereof are stored.

5 In the module  $Mod_{59}$ , the certificate data  $CER_{CP}$  storing the secret key data  $K_{CP,P}$  of the content provider 101, the signature data  $SIG_{ESC}$  by the secret key data  $K_{ESC,S}$  with respect to the certificate data  $CER_{CP}$ , and the data Data to be transmitted are stored.

10 Figure 43H is a view for explaining the data format of the case where the data Data is transmitted from the content provider 101 to the EMD service center 102 by the out-of-band method.

In this case, from the content provider 101 to the  
15 EMD service center 102, a module  $Mod_{60}$  shown in Fig. 43H encrypted by the session key data  $K_{SES}$  obtained by the mutual certification between the content provider 101 and the EMD service center 102 is transmitted.

In the module  $Mod_{60}$ , the data Data to be transmitted  
20 and the signature data  $SIG_{CP}$  by the secret key data  $K_{CP,S}$  thereof are stored.

At this time, the certificate data  $CER_{CP}$  of the content provider 101 has been already registered in the EMD service center 102.

25 Figure 43I is a view for explaining the data format

where the data Data is transmitted from the SAM 105<sub>1</sub> to the EMD service center 102 by the in-band method.

In this case, a module Mod<sub>61</sub> encrypted by the session key data K<sub>SES</sub> obtained by the mutual certification  
5 between the EMD service center 102 and the SAM 105<sub>1</sub> is transmitted from the SAM 105<sub>1</sub> to the EMD service center 102.

In the module Mod<sub>61</sub>, a module Mod<sub>62</sub> and the signature data SIG<sub>SAM1</sub> by the secret key data K<sub>SAM1,S</sub> thereof are  
10 stored.

In the module Mod<sub>62</sub>, the certificate data CER<sub>SAM1</sub> storing the secret key data K<sub>SAM1,P</sub> of the SAM 105<sub>1</sub>, the signature data SIG<sub>ESC</sub> by the secret key data K<sub>ESC,S</sub> with respect to the certificate data CER<sub>SAM1</sub>, and the data Data  
15 to be transmitted are stored.

Figure 43J is a view for explaining the data format where the data Data is transmitted from the SAM 105<sub>1</sub> to the EMD service center 102 by the out-of-band method.

In this case, a module Mod<sub>63</sub> shown in Fig. 43J  
20 encrypted by the session key data K<sub>SES</sub> obtained by the mutual certification between the EMD service center 102 and the SAM 105<sub>1</sub> is transmitted from the SAM 105<sub>1</sub> to the EMD service center 102.

In the module Mod<sub>63</sub>, the data Data to be transmitted  
25 and the signature data SIG<sub>SAM1</sub> by the secret key data K<sub>SAM1,S</sub>

thereof are stored.

At this time, in the EMD service center 102, the certificate data  $CER_{SAM1}$  of the SAM 105<sub>1</sub> has been already registered.

5 Below, an explanation will be made of the registration processing in the EMD service center 102 at the time of shipment of the SAMs 105<sub>1</sub> to 105<sub>4</sub>.

Note that, the registration processings of the SAMs 105<sub>1</sub> to 105<sub>4</sub> are the same, so the registration processing  
10 of the SAM 105<sub>1</sub> will be mentioned below.

At the time of shipment of the SAM 105<sub>1</sub>, by the key server 141 of the EMD service center 102 shown in Fig. 24, the key data shown below is initially registered in the storage unit 192 shown in Fig. 26 etc. via the SAM  
15 management unit 149.

Further, in the SAM 105<sub>1</sub>, for example, at the time of shipment, the program etc. used when accessing the EMD service center 102 by the SAM 105<sub>1</sub> the first time are stored in the storage unit 192 etc.

20 Namely, in the storage unit 192, for example, the identifier  $SAM\_ID$  of the SAM 105<sub>1</sub> given an "\*" at the left side in Fig. 30, storage use key data  $K_{STR}$ , public key data  $K_{R-CA}$  of the route certificate authority 2, public key data  $K_{ESC,P}$  of the EMD service center 102,  
25 secret key data  $K_{SAM1,S}$  of the SAM 105<sub>1</sub>, certificate data

$CER_{SAM1}$  and the signature data  $SIG_{22,ESC}$  thereof, and the original key data for creating the certification use key data between the decryption and/or expansion module 163 and the media SAM are stored by the initial registration.

5        Note that, it is also possible to transmit the certificate data  $CER_{SAM1}$  from the EMD service center 102 to the SAM 105<sub>1</sub> when registering the same after the time of shipment of the SAM 105<sub>1</sub>.

10        Also, in the storage unit 192, at the time of shipment of the SAM 105<sub>1</sub>, a file reader indicating the reading format of the content file CF and the key file KF shown in Fig. 5 is written by the EMD service center 102.

15        In the SAM 105<sub>1</sub>, when utilizing the data stored in the content file CF and the key file KF, the file reader stored in the storage unit 192 is used.

20        Here, the public key data  $K_{R-CA}$  of the route certificate authority 2 uses an RSA generally used in electronic commercial transactions over the Internet and has a data length of for example 1024 bits. The public key data  $K_{R-CA}$  is issued by the route certificate authority 2 shown in Fig. 1.

25        Also, the public key data  $K_{ESC,P}$  of the EMD service center 102 is produced by utilizing an elliptical curve code having a short data length and a power equivalent to the RSA or more. Its data length is for example 160 bits.



Note, when considering the power of the encryption, desirably the public key data  $K_{ESC,P}$  has 192 bits or more. Further, the EMD service center 102 registers the public key data  $K_{ESC,P}$  in the route certificate authority 92.

5       Also, the route certificate authority 92 produces the certificate data  $CER_{ESC}$  of the public key data  $K_{ESC,P}$ . The certificate data  $CER_{ESC}$  storing the public key data  $K_{ESC,P}$  is preferably stored in the storage unit 192 at the time of shipment of the SAM 105<sub>1</sub>. In this case, the  
10       certificate data  $CER_{ESC}$  is signed by a secret key data  $K_{ROOT,S}$  of the route certificate authority 92.

      The EMD service center 102 produces the secret key data  $K_{SAM1,S}$  of the SAM 105<sub>1</sub> by generating a random number and produces the public key data  $K_{SAM1,P}$  forming a pair  
15       together with this.

      Also, the EMD service center 102 is given the certification of the route certificate authority 92, issues the certificate data  $CER_{SAM1}$  of the public key data  $K_{SAM1,P}$ , and attaches the signature data to this by using  
20       its own secret key data  $K_{ESC,S}$ . Namely, the EMD service center 102 achieves the function of a second CA (certificate authority).

      Also, the unique identifier  $SAM\_ID$  under the management of the EMD service center 102 is allocated to  
25       the SAM 105<sub>1</sub> by the SAM management unit 149 of the EMD

service center 102 shown in Fig. 24. This is stored in the storage unit 192 of the SAM 105<sub>1</sub> and, at the same time, stored also in the SAM database 149a shown in Fig. 24 and managed by the EMD service center 102.

5        Also, the SAM 105<sub>1</sub> is connected to and registered at the EMD service center 102 by for example the user after the time of shipment. At the same time, the distribution use public key data KD<sub>1</sub> to KD<sub>3</sub> are transferred from the EMD service center 102 to the storage unit 192.

10        Namely, the user utilizing the SAM 105<sub>1</sub> must perform a registration procedure at the EMD service center 102 before downloading the content. This registration procedure is carried out off-line by for example mail by the user himself giving information specifying himself by  
15        using for example a registration card attached when purchasing the apparatus with the SAM 105<sub>1</sub> mounted thereon (in the related example, network apparatus 160<sub>1</sub>).

      The SAM 105<sub>1</sub> cannot be used until the registration procedure is passed.

20        The EMD service center 102 issues the identifier USER\_ID inherent to the user in accordance with the registration procedure of the SAM 105<sub>1</sub> by the user, manages the correspondence between the SAM\_ID and the USER\_ID in for example the SAM database 149a shown in  
25        Fig. 24, and utilizes the same at the time of charging.

Also, the EMD service center 102 allocates the information reference use identifier ID and the password used at the first time to the user of the SAM 105<sub>1</sub> and notifies this to the user. The user can make an inquiry  
5 about information for example the usage situation (usage log) of the content data up to the present at the EMD service center 102 by using the information reference use identifier ID and the password.

Also, the EMD service center 102 confirms the  
10 identity of the user at the credit card company or the like or confirms the user off-line at the time of registration of the user.

Next, as shown in Fig. 30, an explanation will be made of the procedure for storing the SAM registration  
15 list in the storage unit 192 inside the SAM 105<sub>1</sub>.

The SAM 105<sub>1</sub> shown in Fig. 1 acquires the SAM registration list of the SAMs 105<sub>1</sub> to 105<sub>4</sub> existing in its own system by utilizing a topology map produced when powering up apparatuses connected to the bus 191 and  
20 connecting new apparatuses to the bus 191 where for example the IEEE1394 serial bus is used as the bus 191.

Note that, the topology map produced in accordance with the IEEE1394 serial bus, that is, the bus 191, is produced for the SAMs 105<sub>1</sub> to 105<sub>4</sub> and SCMS processing  
25 circuits 105<sub>5</sub> and 105<sub>6</sub> when, for example, as shown in

Fig. 44, in addition to the SAMs 105<sub>1</sub> to 105<sub>4</sub>, SCMS processing circuits 105<sub>5</sub> and 105<sub>6</sub> of AV apparatus 160<sub>5</sub> and 160<sub>6</sub> are connected to the bus 191.

Accordingly, the SAM 105<sub>1</sub> extracts the information  
5 for the SAMs 105<sub>1</sub> to 105<sub>4</sub> from the related topology map and produces the SAM registration list shown in Fig. 45.

Then, the SAM 105<sub>1</sub> registers the SAM registration list shown in Fig. 45 in the EMD service center 102 and acquires the signature.

10 These processings are automatically carried out by the SAM 105<sub>1</sub> by utilizing the session of the bus 191. The registration instruction of the SAM registration list is issued to the EMD service center 102.

The EMD service center 102 confirms the expiration  
15 date when receiving the SAM registration list shown in Fig. 45 from the SAM 105<sub>1</sub>. Then, the EMD service center 102 sets up the corresponding portion by referring to the existence of the settlement function designated by the SAM 105<sub>1</sub> at the time of registration. Further, the EMD  
20 service center 102 checks the revocation list and sets a revocation flag in the SAM registration list. The revocation list is the list of the SAMs for which usage is prohibited (invalid) by the EMD service center 102 for the reason of for example illegitimate usage.

25 Also, the EMD service center 102 extracts the SAM

registration list corresponding to the SAM 105<sub>1</sub> at the time of settlement and confirms if the SAM described therein is contained in the revocation list. Further, the EMD service center 102 attaches the signature to the SAM registration list.

By this, the SAM registration list shown in Fig. 46 is produced.

Note that, the SAM revocation list is produced aimed at only the SAMs of the identical system (connected to the identical bus 191), and the validity and invalidity of the related SAMs are indicated by the revocation flag corresponding to each SAM.

Below, an explanation will be made of the overall operation of the content provider 101 shown in Fig. 1.

Figure 47 is a flowchart of the overall operation of the content provider 101.

Step S1: The EMD service center 102 transmits the certificate data  $CER_{CP}$  of the public key data  $K_{CP}$  of the content provider 101 to the content provider 101 after the content provider 101 goes through the predetermined registration processing.

Also, the EMD service center 102 transmits the certificate  $CER_{CP1}$  to  $CER_{CP4}$  of the public key data  $K_{SAM1,P}$  to  $K_{SAM4,P}$  of the SAMs 105<sub>1</sub> to 105<sub>4</sub> to the SAMs 105<sub>1</sub> to 105<sub>4</sub> after the SAMs 105<sub>1</sub> to 105<sub>4</sub> pass through the

predetermined registration processing.

Also, the EMD service center 102 transmits three months' worth of the distribution use key data  $KD_1$  to  $KD_3$  each having the expiration date of one month to the SAMs 105<sub>1</sub> to 105<sub>4</sub> of the user home network 103 after the mutual certification.

In this way, in the EMD system 100, the distribution use key data  $KD_1$  to  $KD_3$  are distributed to the SAMs 105<sub>1</sub> to 105<sub>4</sub> in advance. Therefore, even in the state where the space between the SAMs 105<sub>1</sub> to 105<sub>4</sub> and the EMD service center 102 is off-line, the secure container 104 distributed from the content provider 101 can be decrypted and purchased and used in the SAMs 105<sub>1</sub> to 105<sub>4</sub>. In this case, the log of the related purchase and/or usage is described in the usage log data 108, and the usage log data 108 is automatically transmitted to the EMD service center 102 when the SAMs 105<sub>1</sub> to 105<sub>4</sub> and the EMD service center 102 are connected. Therefore, the settlement processing in the EMD service center 102 can be reliably carried out. Note that, a SAM for which usage log data 108 cannot be collected by the EMD service center 102 in a predetermined period is regarded as being invalidated by the revocation list.

Note that, the usage control status data 166 is transmitted from the SAMs 105<sub>1</sub> to 105<sub>4</sub> to the EMD service

center 102 in real-time in principle.

Step S2: The content provider 101 transmits the right registration request module  $Mod_2$  shown in Fig. 18 to the EMD service center 102 after the mutual  
5 certification.

Then, the EMD service center 102 registers and authenticates the usage control policy data 106 and the content key data  $Kc$  after the predetermined signature verification.

10 Also, the EMD service center 102 produces six months' worth of the key files  $KF$  in accordance with the registration use module  $Mod_2$  and transmits them to the content provider 101.

Step S3: The content provider 101 produces the  
15 content files  $CF$  and the signature data  $SIG_{6,CP}$  thereof and the key file  $KF$  and the signature data  $SIG_{7,CP}$  thereof shown in Figs. 5A and 5B and distributes the secure container 104 storing them and the certificate data  $CER_{CP}$  and the signature data  $SIG_{1,ESC}$  thereof shown in Fig. 5C to  
20 the SAMs  $105_1$  to  $105_4$  of the user home network 103 on-line and/or off-line.

In the on-line case, the content provider use transport protocol is used. The secure container 104 is transported from the content provider 101 to the user  
25 home network 103 in a form not depending upon the related

protocol (namely, as data transmitted by using a predetermined layer of communication protocol comprised of a plurality of layers). Also, in the off-line case, the secure container 104 is transported from the content provider 101 to the user home network 103 in the state stored in a ROM type or RAM type storage medium.

Step S4: The SAMs 105<sub>1</sub> to SAM 105<sub>4</sub> of the user home network 103 verify the signature data SIG<sub>6,CP</sub>, SIG<sub>7,CP</sub>, and SIG<sub>KL,ESC</sub> in the secure container 104 distributed from the content provider 101 and confirm the legitimacy of the producer and transmitter of the content file CF and the key file KF, then decrypt the key file KF by using the distribution use data KD<sub>1</sub> to KD<sub>6</sub> of the corresponding period.

Step S5: In the SAMs 105<sub>1</sub> to 105<sub>4</sub>, the purchase and/or usage form is determined based on the operation signal S165 in accordance with the operation of the purchase and/or usage form determination operation unit 165 shown in Fig. 25 by the user.

At this time, in the usage monitor unit 186 shown in Fig. 31, the purchase and/or usage form of the content file CF by the user is managed based on the usage control policy data 106 stored in the secure container 104.

Step S6: In the charge processing unit 187 shown in Fig. 31 of the SAMs 105<sub>1</sub> to 105<sub>4</sub>, the usage log data 108



and the usage control status data 166 describing the operation of the settlement of the purchase and/or usage form by the user are produced based on the operation signal S165 and are transmitted to the EMD service center 102.

Step S7: The EMD service center 102 performs the settlement processing based on the usage log data 108 in the settlement processing unit 142 shown in Fig. 24 and produces the settlement claim data 152 and the settlement report data 107. The EMD service center 102 transmits the settlement claim data 152 and the signature data  $SIG_{88}$  thereof via the payment gateway 90 shown in Fig. 1 to the settlement manager 91. Further, the EMD service center 102 transmits the settlement report data 107 to the content provider 101.

Step S8: In the settlement manager 91, after verifying the signature data  $SIG_{88}$ , based on the settlement claim data 152, the money paid by the user is distributed to the owner of the content provider 101.

As explained above, in the EMD system 100, the secure container 104 of the format shown in Fig. 5 is distributed from the content provider 101 to the user home network 103, and the processing for the key file KF in the secure container 104 is carried out in the SAMs 105<sub>1</sub> to 105<sub>4</sub>.

Also, the content key data  $K_c$  and the usage control policy data 106 stored in the key file  $KF$  have been encrypted by using the distribution use key data  $KD_1$  to  $KD_3$  and decrypted inside only the SAMs  $105_1$  to  $105_4$  holding the distribution use key data  $KD_1$  to  $KD_3$ . Then, in the SAMs  $105_1$  to  $105_4$ , the purchase form and the usage form of the content data  $C$  are determined based on a module having tamper resistance and the handling content of the content data  $C$  described in the usage control policy data 106.

Accordingly, according to the EMD system 100, the purchase and usage of the content data  $C$  in the user home network 103 can be reliably carried out based on the content of the usage control policy data 106 produced by the interested parties of the content provider 101.

Also, in the EMD system 100, by distributing the content data  $C$  from the content provider 101 to the user home network 103 by using the secure container 104 in both of the cases of on-line and off-line, the rights clearing of the content data  $C$  in the SAMs  $105_1$  to  $105_4$  can be shared in both cases.

Also, in the EMD system 100, when purchasing, using, recording, and transferring the content data  $C$  in the network apparatus  $160_1$  and the AV apparatuses  $160_2$  to  $160_4$  in the user home network 103, by performing processing

always based on the usage control policy data 106, common rights clearing rule can be employed.

Figure 48 is a view for explaining an example of the transport protocol of the secure container employed in the first embodiment.

As shown in Fig. 48, in the multi-processor system 100, as the protocol for transporting the secure container 104 from the content provider 101 to the user home network 103, use is made of for example TCP/IP and XML/SMIL.

Also, as the protocol for transferring the secure container between SAMs of the user home network 103, and the protocol for transferring the secure container between the user home networks 103 and 103a, use is made of for example XML/SMIL constructed in the 1394 serial bus interface. Also, in this case, it is also possible to store the secure container in a ROM type or RAM type storage medium and transport the same between SAMs.

First modification of first embodiment

In the above embodiment, as shown in Fig. 5B, the case where the key file KF was encrypted by using the distribution use key data KD in the EMD service center 102, and the key file KF was decrypted by using the distribution use key data KD in the SAMs 105<sub>1</sub> to 105<sub>4</sub>, was exemplified, but the encryption of the key file KF using

the distribution use key data KD does not always have to be carried out when the secure container 104 is directly supplied from the content provider 101 to the SAMs 105<sub>1</sub> to 105<sub>4</sub> as shown in Fig. 1.

5        In this way, the encryption of the key file KF by using the distribution use key data KD has a large effect when suppressing illegitimate action by the service provider by giving the distribution use key data KD to only the content provider and the user home network when  
10    the content data is supplied from the content provider to the user home network via the service provider as in the second embodiment mentioned later.

      Note, also in the case of the first embodiment, the encryption of the key file KF by using the distribution  
15    use key data KD has an effect in the point of raising the force of suppressing illegitimate usage of the content data.

      Further, in the above embodiment, the case where the suggested retailer's price data SRP was stored in the  
20    usage control policy data 106 in the key file KF shown in Fig. 5B was exemplified, but it is also possible to store the suggested retailer's price data SRP (price tag data) other than in the key file KF in the secure container 104. In this case, signature data produced by using the  
25    secret key data  $K_{CP}$  is attached to the suggested

retailer's price data SRP.

Second modification of first embodiment

In the first embodiment, as shown in Fig. 1, the case where the EMD service center 102 performed the settlement processing in the settlement manager 91 via the payment gateway 90 by using the settlement claim data 152 produced by itself was exemplified, but it is also possible to transmit for example the settlement claim data 152 from the EMD service center 102 to the content provider 101 as shown in Fig. 49 and have the content provider 101 itself perform the settlement processing at the settlement manager 91 via the payment gateway 90 by using the settlement claim data 152.

Third modification of first embodiment

In the first embodiment, the case where the secure container 104 was supplied from a single content provider 101 to the SAMs 105<sub>1</sub> to 105<sub>4</sub> of the user home network 103 was exemplified, but it is also possible to supply secure containers 104a and 104b from two or more content providers 101a and 101b to the SAMs 105<sub>1</sub> to 105<sub>4</sub>.

Figure 50 is a view of the configuration of the EMD system according to a third modification of the first embodiment where the content providers 101a and 101b are used.

In this case, the EMD service center 102 distributes

key files KFa<sub>1</sub> to KFa<sub>6</sub> and Kfb<sub>1</sub> to Kfb<sub>6</sub> encrypted by using six months' worth of distribution use key data KDa<sub>1</sub> to KDa<sub>6</sub> and KDb<sub>1</sub> to KDb<sub>6</sub> to the content providers 101a and 101b.

5       Also, the EMD service center 102 distributes three months' worth of distribution use key data KDa<sub>1</sub> to KDa<sub>3</sub> and KDb<sub>1</sub> to KDb<sub>3</sub> to the SAMs 105<sub>1</sub> to 105<sub>4</sub>.

10       Then, the content provider 101a supplies a secure container 104a storing a content file CFa encrypted by using unique content key data Kca and key files KFa<sub>1</sub> to KFa<sub>6</sub> of the corresponding period received from the EMD service center 102 to the SAMs 105<sub>1</sub> to 105<sub>4</sub> on-line and/or off-line.

15       At this time, as the identifier of a key file, use is made of the global unique identifier content ID distributed by the EMD service center 102. The content data is centrally managed by the EMD service center 102.

20       Also, the content provider 101b supplies a secure container 104b storing a content file CFb encrypted by using unique content key data Kcb and key files Kfb<sub>1</sub> to Kfb<sub>6</sub> of the corresponding period received from the EMD service center 102 to the SAMs 105<sub>1</sub> to 105<sub>4</sub> on-line and/or off-line.

25       The SAMs 105<sub>1</sub> to 105<sub>4</sub> decrypt the secure container 104a by using the distribution use key data KDa<sub>1</sub> to KDa<sub>3</sub>

of the corresponding period, determine the purchase form  
of the content after passing through the predetermined  
signature verification processing, etc., and transmit  
usage log data 108a and usage control status data 166a  
5 produced in accordance with the related determined  
purchase form and usage form to the EMD service center  
102.

Also, the SAMs 105<sub>1</sub> to 105<sub>4</sub> decrypt the secure  
container 104b by using the distribution use key data  
10 KDb<sub>1</sub> to KDb<sub>3</sub> of the corresponding period, determine the  
purchase form of the content after passing through the  
predetermined signature verification processing, etc.,  
and transmit usage log data 108b and usage control status  
data 166b produced in accordance with the related  
15 determined purchase form and usage form to the EMD  
service center 102.

In the EMD service center 102, based on the usage  
log data 108a, settlement claim data 152a for the content  
provider 101a is produced, and settlement processing is  
20 carried out at the settlement manager 91 using this.

Also, in the EMD service center 102, settlement  
claim data 152b for the content provider 101b is produced  
based on the usage log data 108b, and settlement  
processing is carried out at the settlement manager 91  
25 using this.

Also, the EMD service center 102 registers and authenticates the usage control policy data 106a and 106b. At this time, the EMD service center 102 distributes the global unique identifier content ID for the key files KFa and KFb corresponding to the usage control policy data 106a and 106b.

Also, the EMD service center 102 issues certificate data  $CER_{CPa}$  and  $CER_{CPb}$  of the content providers 101a and 101b and attaches signature data  $SIG_{1b,ESC}$  and  $SIG_{1a,ESC}$  to them to verify their legitimacy.

Fourth modification of first embodiment

In the above embodiment, the case where the content files CF and the key files KF were stored in the secure container 104 with directory structures and transmitted from the content provider 101 to the SAMs 105<sub>1</sub> to 105<sub>4</sub> was exemplified, but it is also possible to separately transmit the content files CF and the key file KF to the SAMs 105<sub>1</sub> to 105<sub>4</sub>.

This includes for example the following first technique and second technique.

In the first technique, as shown in Fig. 52, the content files CF and the key files KF are separately transmitted from the content provider 101 to the SAMs 105<sub>1</sub> to 105<sub>4</sub> in a format not depending upon the communication protocol.



Also, in the second technique, as shown in Fig. 52, the content files CF are transmitted from the content provider 101 to the SAMs 105<sub>1</sub> to 105<sub>4</sub> in a format not depending upon the communication protocol and, at the same time, the key files KF are transmitted from the EMD service center 102 to the SAMs 105<sub>1</sub> to 105<sub>4</sub>. The related key files KF are transmitted from the EMD service center 102 to the SAMs 105<sub>1</sub> to 105<sub>4</sub> when for example the users of the SAMs 105<sub>1</sub> to 105<sub>4</sub> are about to determine the purchase form of the content data C.

When the first technique and the second technique are employed, a link is established between related content files CF and between the content files CF and the key files KF corresponding to them by using hyper link data stored in the header of at least one of the content file CF and the key file KF. In the SAMs 105<sub>1</sub> to 105<sub>4</sub>, the rights clearing and the usage of the content data C are carried out based on the related link.

Note that, in the present modification, as the formats of the content file CF and the key file KF, for example, those shown in Figs. 5A and 5B are employed. Also, in this case, preferably, together with the content file CF and the key file KF, the signature data SIG<sub>6,CP</sub> and SIG<sub>7,CP</sub> thereof are transmitted.

Fifth modification of first embodiment

In the above embodiment, the case where the content file CF and the key file KF were separately provided in the secure container 104 was exemplified, but for example it is also possible to store the key file KF in the content file CF in the secure container 104 as shown in Fig. 53.

In this case, the signature data by the secret key data  $K_{CP,S}$  of the content provider 101 is attached to the content file CF storing the key file KF.

10      Sixth modification of first embodiment

In the above embodiment, the case where the content data C was stored in the content file CF, and the content key data Kc and the usage control policy data 106 were stored in the key file KF and transmitted from the content provider 101 to the SAM 105<sub>1</sub> or the like was exemplified, but it is also possible to transmit at least one among the content data C, content key data Kc, and the usage control policy data 106 from the content provider 101 to the SAM 105<sub>1</sub> or the like without employing the file format and in a format not depending upon the communication protocol.

For example, as shown in Fig. 54, it is also possible if a secure container 104s storing the key file KF containing the content data C encrypted by the content key data Kc, the encrypted content key data Kc, the

encrypted usage control policy data 106, etc. is produced in the content provider 101, and the secure container 104s is transmitted to the SAM 105<sub>1</sub> etc. in a format not depending upon the communication protocol.

5       Also, as shown in Fig. 55, it is also possible to individually transmit the key file KF containing the content data C encrypted by the content key data Kc, encrypted content key data Kc, the encrypted usage control policy data 106, and so on from the content  
10 provider 101 to the SAM 105<sub>1</sub> etc. in a format not depending upon the communication protocol. Namely, the content data C is transmitted by an identical route to the key file KF without employing the file format.

Also, as shown in Fig. 56, it is also possible if  
15 the content data C encrypted by the content key data Kc is transmitted from the content provider 101 to the SAM 105<sub>1</sub> etc. in a format not depending upon the communication protocol and, at the same time, the key file KF containing the encrypted content key data Kc and  
20 the encrypted usage control policy data 106 etc. is transmitted from the EMD service center 102 to the SAM 105<sub>1</sub> etc. Namely, the content data C is transmitted by a different route from that for the key file KF without employing the file format.

25       Also, as shown in Fig. 57, it is also possible if

the content data C encrypted by the content key data Kc,  
the content key data Kc, and the usage control policy  
data 106 are transmitted from the content provider 101 to  
the SAM 105<sub>1</sub> etc. in a format not depending upon the  
5 communication protocol. Namely, the content data C,  
content key data Kc, and the usage control policy data  
106 are transmitted by the identical route without  
employing the file format.

Also, as shown in Fig. 58, it is also possible if  
10 the content data C encrypted by the content key data Kc  
is transmitted from the content provider 101 to the SAM  
105<sub>1</sub> etc. in a format not depending upon the  
communication protocol and, at the same time, the content  
key data Kc and the usage control policy data 106 are  
15 transmitted from the EMD service center 102 to the SAM  
105<sub>1</sub> etc. Namely, the content data C, content key data  
Kc, and the usage control policy data 106 are transmitted  
by different routes without employing the file format.

#### Second embodiment

20 In the above embodiment, the case where the content  
data was directly distributed from the content provider  
101 to the SAMs 105<sub>1</sub> to 105<sub>4</sub> of the user home network 103  
was exemplified, but in the present embodiment, an  
explanation will be made of a case where the content data  
25 provided by the content provider is distributed to a SAM

of the user home network via the service provider.

Figure 59 is a view of the configuration of an EMD system 300 of the present embodiment.

As shown in Fig. 59, the EMD system 300 has a  
5 content provider 301, an EMD service center 302, the user home network 303, a service provider 310, the payment gateway 90, and the settlement manager 91.

The content provider 301, EMD service center 302, SAMs 305<sub>1</sub> to 305<sub>4</sub>, and the service provider 310  
10 correspond to the data providing apparatus, management device, data processing apparatus, and the data distribution apparatus according to claim 22 and claim 152 etc.

The content provider 301 is the same as the content  
15 provider 101 of the first embodiment except for the point that it supplies the content data to the service provider 310.

Also, the EMD service center 302 is the same as the EMD service center 102 of the first embodiment except for  
20 the point that the certificate authority function, key data management function, and the rights clearing function are provided also to the service provider 310 in addition to the content provider 101 and SAMs 505<sub>1</sub> to 505<sub>4</sub>.

25 Also, the user home network 303 has a network

apparatus 360<sub>1</sub> and AV apparatuses 360<sub>2</sub> to 360<sub>4</sub>. The network apparatus 360<sub>1</sub> includes a SAM 305<sub>1</sub> and a CA module 311, and the AV apparatuses 360<sub>2</sub> to 360<sub>4</sub> include the SAMs 305<sub>2</sub> to 305<sub>4</sub>.

5        Here, the SAMs 305<sub>1</sub> to 305<sub>4</sub> are the same as the SAMs 105<sub>1</sub> to 105<sub>4</sub> of the first embodiment except for the point that they are distributed a secure container 304 from the service provider 310 and the point that they perform the verification processing of the signature data and the  
10       preparation of an SP use purchase log data (data distribution device use purchase log data) 309 for the service provider 310 in addition to the content provider 301.

15       First, a brief explanation will be made of the EMD system 300.

      In the EMD system 300, the content provider 301 transmits the usage control policy (UCP) data 106 in the same way as that of the first embodiment mentioned before indicating the rights contents such as the usage  
20       permission condition of the content data C of the content to be provided by itself and the content key data Kc to the EMD service center 302 as the authority manager having a high reliability. The usage control policy data 106 and the content key data Kc are registered and  
25       authenticated (certified) in the EMD service center 302.

Also, the content provider 301 encrypts the content data C by the content key data Kc and produces the content file CF. Also, the content provider receives six months' worth of the key files KF for the content files CF from the EMD service center 302.

In the related key file KF, the signature data for verifying the existence of tampering of the related key file KF and the legitimacy of the producer and the transmitter of the related key file KF is stored.

Then, the content provider 301 supplies the secure container 104 shown in Fig. 5 storing the content file CF, key file KF, and its own signature data to the service provider 310 by using a network such as the Internet, digital broadcast, storage medium, or informal protocol or off-line or the like.

Also, the signature data stored in the secure container 104 is used for verifying the existence of tampering of the corresponding data and the legitimacy of the producer and transmitter of the related data.

When receiving the secure container 104 from the content provider 301, the service provider 310 verifies the signature data and confirms the producer and the transmitter of the secure container 104.

Next, the service provider 310 produces price tag data (PT) 312 indicating the price obtained by adding a

price for service such as authoring performed by itself to the price (SRP) for the content intended by the content provider 301 notified for example off-line.

Then, the service provider 310 produces the secure  
5 container 304 storing the content file CF and key file KF extracted from the secure container 104, price tag data 312, and the signature data by its own secret key data  $K_{SP,S}$  with respect to them.

At this time, the key file KF has been encrypted by  
10 the distribution use key data  $KD_1$  to  $KD_6$ , and the service provider 310 does not hold the related distribution use key data  $KD_1$  to  $KD_6$ , therefore the service provider 310 cannot see or rewrite the content of the key file KF.

Also, the EMD service center 302 registers and  
15 authenticates the price tag data 312.

The service provider 310 distributes the secure container 304 to the user home network 303 on-line and/or off-line.

At this time, in the case of off-line, the secure  
20 container 304 is stored in the ROM type storage medium or the like and supplied to the SAMs 305<sub>1</sub> to 305<sub>4</sub> as it is. On the other hand, in the case of on-line, mutual certification is carried out between the service provider 310 and the CA module 311, the secure container 304 is  
25 encrypted by using the session key data  $K_{SES}$  in the



service provider 310 and transmitted, and the secure container 304 received at the CA module 311 is decrypted by using the session key data  $K_{SES}$  and then transferred to the SAMs 305<sub>1</sub> to 305<sub>4</sub>.

5        In this case, as the communication protocol for transmitting the secure container 304 from the content provider 301 to the user home network 303, an MHEG (Multimedia and Hypermedia Information Coding Experts Group) protocol is used in the case of a digital  
10       broadcast and XML/SMIL/HTML (Hyper Textmarkup Language) is used in the case of the Internet. In these communication protocols, the secure container 304 is buried by tunneling in a format not depending upon the related communication protocol (encoding method or the  
15       like).

Accordingly, it is not necessary to ensure compatibility of the format between the communication protocol and the secure container 304, so the format of the secure container 304 can be flexibly set.

20       Next, in the SAMs 305<sub>1</sub> to 305<sub>4</sub>, the signature data stored in the secure container 304 is verified, and the legitimacy of producers and transmitters of the content file CF and the key file KF stored in the secure container 304 is confirmed. Then, in the SAMs 305<sub>1</sub> to  
25       305<sub>4</sub>, when the related legitimacy is confirmed, the key

file KF is decrypted by using the distribution use data  
KD<sub>1</sub> to KD<sub>3</sub> of the corresponding period distributed from  
the EMD service center 302.

The secure container 304 supplied to the SAMs 305<sub>1</sub>  
5 to 305<sub>4</sub> is reproduced and recorded into the storage  
medium after the purchase and/or usage form is determined  
in accordance with the operation of the user in the  
network apparatus 360<sub>1</sub> and the AV apparatuses 360<sub>2</sub> to  
360<sub>4</sub>.

10 The SAMs 305<sub>1</sub> to 305<sub>4</sub> store the log of the purchase  
and/or usage of the secure container 304 as the usage log  
data 308.

A usage log data (log data or the management device  
use log data) 308 is transmitted from the user home  
15 network 303 to the EMD service center 302 in response to  
for example a request from the EMD service center 302.

Also, the SAMs 305<sub>1</sub> to 305<sub>4</sub> transmit the usage  
control status (UCS) data 166 indicating the related  
purchase form to the EMD service center 302 when the  
20 purchase form of the content is determined.

The EMD service center 302 determines (calculates)  
the charge content for each of the content provider 301  
and the service provider 310 based on the usage log data  
308 and performs settlement at the settlement manager 91  
25 such as a bank via the payment gateway 90 based on the

results. By this, the money paid by the user of the user home network 103 is distributed to the content provider 101 and the service provider 310 by the settlement processing by the EMD service center 102.

5 In the present embodiment, the EMD service center 302 has the certificate authority function, key data management function, and the rights clearing (profit distribution) function.

10 Namely, the EMD service center 302 functions as a second certificate authority with respect to the route certificate authority 92 as the highest authority manager at the neutral position and verifies the legitimacy of the related public key data by attaching a signature by the secret key data of the EMD service center 302 to the  
15 certificate data of the public key data to be used for the verification processing of the signature data in the content provider 301, service provider 310, and the SAMs 305<sub>1</sub> to 305<sub>4</sub>. Further, as mentioned before, also the registration and authentication of the usage control  
20 policy data 106 of the content provider 301, content key data Kc, and the price tag data 312 of the service provider 310 are achieved by the certificate authority function of the EMD service center 302.

Also, the EMD service center 302 has a key data  
25 management function for performing for example management

of the key data of the distribution use key data  $KD_1$  to  $KD_6$ .

Also, the EMD service center 302 has a rights clearing (profit distribution) function of performing settlement with respect to the purchase and/or usage of the content by the user of the user home network 303 based on the usage control policy data 106 registered by the content provider 301, the usage log data 308 input from the SAMs 305<sub>1</sub> to 305<sub>4</sub>, and the price tag data 312 registered by the service provider 310 and distributing and paying the money paid by the user to the content provider 301 and the service provider 310.

Below, components of the content provider 301 will be explained in detail.

[Content provider 301]

Figure 60 is a functional block diagram of the content provider 301 and shows the flow of the data related to the data transmitted and received with the service provider 310.

As shown in Fig. 60, the content provider 301 has a content master source server 111, electronic watermark information addition unit 112, compression unit 113, encryption unit 114, random number generation unit 115, signature processing unit 117, secure container preparation unit 118, secure container database 118a, key

file database 118b, storage unit 119, mutual  
certification unit 120, encryption and/or decryption unit  
121, usage control policy data preparation unit 122, EMD  
service center management unit 125, and a service  
5 provider management unit 324.

In Fig. 60, components given the same reference  
numerals as those of Fig. 3 are the same as the  
components of the same reference numerals explained in  
the first embodiment referring to Fig. 3 and Fig. 4.

10 Namely, the content provider 301 has a configuration  
providing the service provider management unit 324 in  
place of the SAM management unit 124 shown in Fig. 3.

The service provider management unit 324 provides  
the secure container 104 shown in Fig. 5 input from the  
15 secure container preparation unit 118 to the service  
provider 310 shown in Fig. 59 off-line and/or on-line.

Where the secure container 104 shown in Fig. 5 is  
distributed to the service provider 310 on-line, the  
service provider management unit 324 encrypts the secure  
20 container 104 by using the session key data  $K_{SES}$  in the  
encryption and/or decryption unit 121 and then  
distributes the same via the network to the service  
provider 310.

Also, the flow of the data in the content provider  
25 101 shown in Fig. 4 similarly applies also to the content

provider 301.

Below, an explanation will be made of the flow of the processing when transmitting the secure container 104 from the content provider 301 to the service provider

5 310.

Figure 61 and Fig. 62 are flowcharts showing the flow of the processing when transmitting the secure container 104 from the content provider 301 to the service provider 310.

10 Step C1: Mutual certification is carried out between the content provider 301 and the service provider 310.

Step C2: The session key data  $K_{SES}$  obtained by the mutual certification at step C1 is shared between the content provider 301 and the service provider 310.

15 Step C3: By the service provider 310, the secure container database 118a possessed by the content provider 301 (for CP) is accessed.

Step C4: The service provider 310 selects the secure container 104 necessary for its distribution service by referring to for example the lists of the content ID and the meta data centrally managed at the secure container database 118a.

20 Step C5: The content provider 301 encrypts the secure container 104 selected at step C4 by using the session key data  $K_{SES}$  shared at step C2.

25

Step C6: The content provider 301 inserts the secure container 104 obtained at step C5 into a content provider use commodity transport protocol.

5      Step C7: The service provider 310 performs the download.

Step C8: The service provider 310 takes out the secure container 104 from the content provider use commodity transport protocol.

10      Step C9: The service provider 310 decrypts the secure container 104 by using the session key data  $K_{SES}$  shared at step C2.

15      Step C10: The service provider 310 verifies the signature data stored in the decrypted secure container 104 to confirm the legitimacy of the transmitter and performs the processing of step C11 under the condition that the transmitter is legitimate.

Step C11: The service provider 310 stores the secure container 104 in the secure container database of itself.

[Service provider 310]

20      The service provider 310 produces the secure container 304 storing the content file CF and the key file KF in the secure container 104 received from the content provider 301 and the price tag data 312 produced by itself and distributes the secure container 304 to the  
25      network apparatus 360<sub>1</sub> and the AV apparatuses 360<sub>2</sub> to 360<sub>4</sub>

of the user home network 303 on-line and/or off-line.

The service format of the content distribution by the service provider 310 is roughly classified to an independent type service and a linked type service.

5       The independent type service is for example a service dedicated to download for individually distributing the content. Further, the linked type service is a service for distributing content linked to the program and CMs (advertisements). For example,  
10       content such as a theme song and other song of a drama are stored in a stream of the drama program. The user can purchase the content such as theme song or other song existing in the stream when watching the drama program.

Figure 63 is a functional block diagram of the  
15       service provider 310.

Note that, in Fig. 63, the flow of the data when supplying the secure container 304 produced by using the secure container 104 supplied from the content provider 301 to the user home network 303 is shown.

20       As shown in Fig. 63, the service provider 310 has a content provider management unit 350, a storage unit 351, a mutual certification unit 352, an encryption and/or decryption unit 353, a signature processing unit 354, a secure container preparation unit 355, a secure container  
25       database 355a, a price tag data preparation unit 356, a



user home network management unit 357, an EMD service center management unit 358, and a user preference filter generation unit 920.

Below, an explanation will be made of the flow of the processing in the service provider 310 when creating the secure container 304 from the secure container 104 supplied from the content provider 301 and distributing this to the user home network 303 by referring to Fig. 63 and Fig. 64.

Figure 64 is a flowchart for explaining the processing of distributing the secure container 304 from the content provider 301 to the service provider 310.

<Step D1>

The content provider management unit 350 receives the secure container 104 shown in Fig. 5 from the content provider 301 on-line and/or off-line and writes the secure container 104 into the storage unit 351.

At this time, the content provider management unit 350 decrypts the secure container 104 in the encryption and/or decryption unit 353 by using the session key data  $K_{SES}$  obtained by mutual certification between the mutual certification unit 120 shown in Fig. 60 and the mutual certification unit 352 shown in Fig. 63 in the case of on-line and then writes the same into the storage unit 351.

Note that, the service provider 310 can have a dedicated secure container database for storing the secure container 104 separately from the storage unit 351.

5       <Step D2>

Next, in the signature processing unit 354, the signature data  $SIG_{1,ESC}$  shown in Fig. 5C of the secure container 104 stored in the storage unit 351 is verified by using the public key data  $K_{ESC,P}$  of the EMD service center 302 read out from the storage unit 351. After the legitimacy thereof is confirmed, the public key data  $K_{CP,P}$  is extracted from the certificate data  $CER_{CP}$  shown in Fig. 5C.

Next, the signature processing unit 354 verifies the signature data  $SIG_{6,CP}$  and  $SIG_{7,CP}$  shown in Figs. 5A and 5B of the secure container 104 stored in the storage unit 351, that is, verifies the legitimacy of the producer and transmitter of the content file CF and the transmitter of the key file KF by using the related extracted public key data  $K_{CP,P}$ .

Also, the signature processing unit 354 verifies the signature data  $SIG_{K1,ESC}$  stored in the key file KF shown in Fig. 5B by using the public key data  $K_{ESC,P}$  read out from the storage unit 351, that is, verifies the legitimacy of the producer of the key file KF. At this time, the

verification of the signature data  $SIG_{K1,ESC}$  serves also as the verification of whether or not the key file KF is registered in the EMD service center 302.

<Step D3>

5       Next, the secure container preparation unit 355 reads out the content file CF and the signature data  $SIG_{6,CP}$  thereof, the key file KF and the signature data  $SIG_{7,CP}$  thereof, the certificate data  $CER_{SP}$  of the service provider 310 and the signature data  $SIG_{61,ESC}$  thereof, and  
10   the certificate data  $CER_{CP}$  of the content provider 301 and the signature data  $SIG_{1,ESC}$  thereof from the storage unit 351 when the legitimacy of the signature data  $SIG_{6,CP}$ ,  $SIG_{7,CP}$  and  $SIG_{K1,ESC}$  is confirmed.

      Also, the price tag data preparation unit 356  
15   produces price tag data 312 indicating the price obtained by adding the price of its own service to the price for the content requested by the content provider 301 notified from for example the content provider 301 off-line and stores this in the storage unit 351.

20       Also, the signature processing unit 354 obtains the hash values of the content file CF, key file KF, and the price tag data 312, produces signature data  $SIG_{62,SP}$ ,  $SIG_{63,SP}$ , and  $SIG_{64,SP}$  by using secret key data  $K_{SP,P}$  of the service provider 310, and outputs them to the secure  
25   container preparation unit 355.

Here, the signature data  $SIG_{62,SP}$  is used for verifying the legitimacy of the transmitter of the content file CF, the signature data  $SIG_{63,SP}$  is used for verifying the legitimacy of the transmitter of the key file KF, and the signature data  $SIG_{64,SP}$  is used for verifying the legitimacy of the producer and transmitter of the price tag data 312.

Next, the secure container preparation unit 355 produces the secure container 304 storing the content file CF and the signature data  $SIG_{6,CP}$  and  $SIG_{62,SP}$  thereof, the key file KF and the signature data  $SIG_{7,CP}$  and  $SIG_{63,ESC}$  thereof, the price tag data 312 and the signature data  $SIG_{64,SP}$  thereof, the certificate data  $CER_{SP}$  and the signature data  $SIG_{61,ESC}$  thereof, and the certificate data  $CER_{CP}$  and the signature data  $SIG_{1,ESC}$  thereof as shown in Figs. 65A to 65D and stores the same in the secure container database 355a.

The secure containers 304 stored in the secure container database 355a are centrally managed by the service provider 310 by using for example content IDs.

<Step D4>

The secure container preparation unit 355 reads out the secure container 304 in response to the request from the user home network 303 from the secure container database 355a and outputs this to the user home network

management unit 357.

At this time, the secure container 304 may be a composite container storing a plurality of content files CF and a plurality of key files KF corresponding to them too. For example, it is also possible to store a plurality of content files CF concerning a song, a video clip, a text card, liner notes, and a jacket in a single secure container 304. It is also possible if these plurality of content files CF etc. are stored in the secure container 304 with a directory structure.

Also, where the secure container 304 is transmitted in a digital broadcast, an MHEG (Multimedia and Hypermedia Information Coding Experts Group) protocol is used, while where it is transmitted by the Internet, an XML/SMIL/HTML (Hyper Text Markup Language) protocol is used.

At this time, the content files CF and the key files KF etc. in the secure container 304 are stored in predetermined layers in the communication protocol employed between the service provider 310 and the user home network 303 in a format not depending upon the encoding method tunneling the protocols of MHEG and HTML.

For example, where the secure container 304 is transmitted in a digital broadcast, as shown in Fig. 66, the content file CF is stored as the MHEG content data in

the MHEG object.

Also, in the transport layer protocol, the MHEG object is stored in PES (packetized elementary stream)- Video in the case of a moving picture image, stored in the PES-Audio in the case of audio, and stored in Private-Data in the case of a still image.

Also, as shown in Fig. 67, the key file KF, price tag data 312, and the certificate data  $CER_{CP}$  and  $CER_{SP}$  are stored in an ECM (entitlement control message) in TS Packet of the transport layer protocol.

Here, a mutual link is established among the content file CF, key file KF, price tag data 312, and the certificate data  $CER_{CP}$  and  $CER_{SP}$  by the directory structure data  $DSD_1$  in the header of the content file CF.

Next, the user home network management unit 357 supplies the secure container 304 to the user home network 303 off-line and/or on-line.

Where the secure container 304 is to be distributed to the network apparatus 360<sub>1</sub> of the user home network 303 on-line, the user home network management unit 357 encrypts the secure container 304 by using the session key data  $K_{SES}$  in the encryption and/or decryption unit 352 after the mutual certification and then distributes the same via the network to the network apparatus 360<sub>1</sub>.

Note that, where the secure container 304 is to be

broadcasted via for example a satellite, the user home network management unit 357 encrypts the secure container 304 by using scramble key data  $K_{SCR}$  or the like. Further, scramble key data  $K_{SCR}$  is encrypted by using work key data  $K_W$ , and the work key data  $K_W$  is encrypted by using master key data  $K_M$ .

Then, the user home network management unit 357 transmits scramble key data  $K_{SCR}$  and the work key data  $K_W$  together with the secure container 304 to the user home network 303 via the satellite.

Also, for example it stores the master key data  $K_M$  in the IC card or the like and distributes the same to the user home network 303 off-line.

Also, when receiving the SP use purchase log data 309 concerning the content data C distributed by the related service provider 310 from the user home network 303, the user home network management unit 357 writes this into the storage unit 351.

The service provider 310 refers to the SP use purchase log data 309 when determining the service content in the future. Further, the user preference filter generation unit 920 analyzes the preference of the users of the SAMs 305<sub>1</sub> to 305<sub>4</sub>, transmitting the related SP use purchase log data 309 based on the SP use purchase log data 309 to produce user preference filter data 900

and transmits this via the user home network management unit 357 to the CA module 311 of the user home network 303.

In Fig. 68, the flow of the data related to the communication with the EMD service center 302 in the service provider 310 is shown.

Note that, as the prerequisite of performing the following processing, the interested party of the service provider 310 performs registration processing at the EMD service center 302 off-line by using for example its own ID card and a bank account for performing the settlement processing and acquires the global unique identifier SP\_ID. The identifier SP\_ID is stored in the storage unit 351.

First, an explanation will be made of the processing where the service provider 310 requests the certificate data  $CER_{SP}$  for certifying the legitimacy of the public key data  $K_{SP,S}$  corresponding to its own secret key data  $K_{SP,S}$  at the EMD service center 302 by referring to Fig. 54.

The service provider 310 generates a random number by using the true random number generator to produce the secret key data  $K_{SP,S}$ , produces the public key data  $K_{SP,S}$  corresponding to the related secret key data  $K_{SP,S}$ , and stores the same in the storage unit 351.



The identifiers  $SP\_ID$  and the public key data  $K_{SP,P}$  of the EMD service center management unit 358 and the service provider 310 are read out from the storage unit 351.

5        Then, the EMD service center management unit 358 transmits the identifier  $SP\_ID$  and the public key data  $K_{SP,P}$  to the EMD service center 302.

10        Then, the EMD service center management unit 348 receives as its inputs the certificate data  $CER_{SP}$  and the signature data  $SIG_{61,ESC}$  thereof from the EMD service center 302 in accordance with the related registration and writes the same into the storage unit 351.

15        Next, an explanation will be made of the processing of the case where the service provider 310 registers and authenticates the price tag data 312 in the EMD service center 302 by referring to Fig. 54.

20        In this case, in the signature processing unit 354, the hash value of a module  $Mod_{103}$  shown in Fig. 69 storing the price tag data 312 read out from the storage unit 351 and the content ID as the global unique identifier is found, and signature data  $SIG_{80,SP}$  is produced by using the secret key data  $K_{SP,S}$ .

25        Also, the certificate data  $CER_{SP}$  and the signature data  $SIG_{61,ESC}$  thereof are read out from the storage unit 351.

Then, after encrypting a price tag registration request use module  $\text{Mod}_{102}$  shown in Fig. 69 by using the session key data  $K_{\text{SES}}$  obtained by the mutual certification between the mutual certification unit 352 and the EMD service center 302 in the encryption and/or decryption unit 353, it is transmitted from the EMD service center management unit 358 to the EMD service center 302.

Note that, it is also possible if the global unique identifier  $\text{SP\_ID}$  of the service provider 310 is stored in the module  $\text{Mod}_{102}$ .

Also, the EMD service center management unit 358 writes a settlement report data 307s received from the EMD service center 302 into the storage unit 351.

Also, the EMD service center management unit 358 stores marketing information data 904 received from the EMD service center 302 in the storage unit 351.

The marketing information data 904 is used as a reference when the service provider 310 determines the content data C to be distributed from then on.

[EMD service center 302]

The EMD service center 302 functions as the certificate authority (CA), key management authority, and the rights clearing authority as mentioned before.

Figure 70 is a view of the configuration of the EMD service center 302.

As shown in Fig. 70, the EMD service center 302 has a key server 141, a key database 141a, a KF preparation unit 153, a settlement processing unit 442, a signature processing unit 443, a settlement manager management unit 144, a certificate and usage control policy management unit 445, a CER database 445a, a certificate database 445b, a content provider management unit 148, a CP database 148a, a SAM management unit 149, a SAM database 149a, a mutual certification unit 150, an encryption and/or decryption unit 151, a service provider management unit 390, an SP database 390a, a content ID preparation unit 851, a user preference filter generation unit 901, and a marketing information data generation unit 902.

In Fig. 70, the functional blocks given the same reference numerals as those of Fig. 23 and Fig. 24 have substantially the same functions as those of the functional blocks having the same reference numerals explained in the first embodiment.

Below, an explanation will be made of the functional blocks given the new reference numerals in Fig. 70.

Note that, in Fig. 70, the flow of the data related to the data transmitted and received between the EMD service center 302 and the service provider 310 in the flow of the data among the functional blocks in the EMD service center 302 is shown.

Further, in Fig. 71, the flow of the data related to the data transmitted and received between the EMD service center 302 and the content provider 301 in the flow of the data among the functional blocks in the EMD service center 302 is shown.

Further, in Fig. 72, the flow of the data related to the data transmitted and received between the EMD service center 302 and the SAMs 305<sub>1</sub> to 305<sub>4</sub> shown in Fig. 59 and the settlement manager 91 in the flow of the data among the functional blocks in the EMD service center 302 is shown.

The settlement processing unit 442 performs the settlement processing based on the usage log data 308 input from the SAMs 305<sub>1</sub> to 305<sub>4</sub> and the suggested retailer's price data SPR and the price tag data 312 input from the certificate and usage control policy management unit 445 as shown in Fig. 72. Note that, at this time, the settlement processing unit 442 monitors the existence of dumping etc. by the service provider 310.

The settlement processing unit 442 produces settlement report data 307c and settlement claim data 152c for the content provider 301 as shown in Fig. 72 by the settlement processing and outputs them to the content provider management unit 148 and the settlement manager

management unit 144.

Also, by the settlement processing, as shown in Fig. 70 and Fig. 72, the settlement report data 307s and settlement claim data 152s for the service provider 310 are produced and are output to the service provider management unit 390 and the settlement manager management unit 144.

Here, the settlement claim data 152c and 152s are authenticated data enabling claim of payment of money to the settlement manager 91 based on the related data.

Here, the usage log data 308 is used when determining the payment of the license fee related to the secure container 304 in the same way as the usage log data 108 explained in the first embodiment. In the usage log data 308, for example, as shown in Fig. 73, the identifier of the content data C stored in the secure container 304, that is, the content ID, the identifier CP\_ID of the content provider 301 providing the content data C stored in the secure container 304, the identifier SP\_ID of the service provider 310 distributing the secure container 304, signal parameter data of the content data C, the compression method of the content data C in the secure container 304, the identifier Media\_ID of the storage medium storing the secure container 304, the identifiers SAM\_ID of the SAMs 305<sub>1</sub> to 305<sub>4</sub>, receiving the

distribution of the secure container 304, the USER\_IDs of the users of the related SAMs 105<sub>1</sub> to 105<sub>4</sub>, etc. are described. Accordingly, in a case where the money paid by the user of the user home network 303 must be distributed to the license owners of for example the compression method and the storage medium other than the owners of the content provider 301 and the service provider 310, the EMD service center 302 determines the sum of money to be paid to the other parties based on the distribution rate table determined in advance and produces the settlement report data and settlement claim data in accordance with the related determination.

The certificate and usage control policy management unit 445 reads out the certificate data CER<sub>CP</sub>, certificate data CER<sub>SP</sub>, the certificate data CER<sub>SAM1</sub> to CER<sub>SAM2</sub>, etc. registered and authenticated in the certificate database 445b and, at the same time, registers and authenticates the usage control policy data 106 and content key data Kc of the content provider 301, the price tag data 312 of the service provider 310, etc. in the CER database 445a.

At this time, the certificate and usage control policy management unit 445 obtains the hash values of the usage control policy data 106, content key data Kc, the price tag data 312, etc., attaches the signature data

using the secret key data  $K_{ESC,S}$ , and produces the authenticated certificate data.

The content provider management unit 148 has a function of communicating with the content provider 101 and can access the CP database 148a for managing the registered identifier CP\_ID etc. of the content provider 101.

The user preference filter generation unit 901 produces user preference filter data 903 for selecting the content data C in accordance with the preference of the users of the SAMs 305<sub>1</sub> to 305<sub>4</sub>, transmitting the related usage log data 308 based on the usage log data 308 and transmits the user preference filter data 903 to the SAMs 305<sub>1</sub> to 305<sub>4</sub>, transmitting the related usage log data 308 via the SAM management unit 149.

The marketing information data generation unit 902 produces the marketing information data 904 indicating the purchase situation etc. of the whole content data C distributed to the user home network 103 by for example a plurality of service providers 310 based on the usage log data 308 and transmits this via the service provider management unit 390 to the service provider 310. The service provider 310 determines the content of the service to be provided from then on with reference to the marketing information data 904.

Below, an explanation will be made of the flow of the processing in the EMD service center 302.

The distribution use key data  $KD_1$  to  $KD_3$  are transmitted from the EMD service center 302 to the SAMs 5 305<sub>1</sub> to 305<sub>4</sub> in the same way as the case of the first embodiment.

Also, the processing in the case where the EMD service center 302 receives the issuance request of the certificate data from the content provider 301 is the 10 same as the first embodiment except for the point that the certificate and usage control policy management unit 445 accesses the certificate database 445b. Further, the processing of registering the usage control policy data 106 etc. is similar to the case of the first embodiment 15 mentioned above except for the point that the certificate and usage control policy management unit 445 stores the related data in the CER database 445a.

Next, an explanation will be made of the processing in the case where the EMD service center 302 receives the 20 issuance request of the certificate data from the service provider 310 by referring to Fig. 70.

In this case, when receiving the identifier  $SP\_ID$ , public key data  $K_{SP,P}$ , and signature data  $SIG_{70,SP}$  of the service provider 310 given by the EMD service center 302 25 in advance from the service provider 310, the service



provider management unit 390 decrypts them by using the session key data  $K_{SES}$  obtained by the mutual certification between the mutual certification unit 150 and the mutual certification unit 352 shown in Fig. 63.

5        Then, after confirming the legitimacy of the related decrypted signature data  $SIG_{70,SP}$  at the signature processing unit 443, it is confirmed whether or not the service provider 310 issuing the issuance request of the related certificate data is registered in the SP database  
10    390a based on the identifier  $SP\_ID$  and the public key data  $K_{SP,P}$ .

Then, the certificate and usage control policy management unit 445 reads out the certificate data  $CER_{SP}$  of the related service provider 310 from the certificate  
15    database 445b and outputs the same to the service provider management unit 390.

Also, the signature processing unit 443 obtains the hash value of the certificate data  $CER_{SP}$ , produces the signature data  $SIG_{61,ESC}$  by using the secret key data  $K_{ESC,S}$   
20    of the EMD service center 302, and outputs this to the service provider management unit 390.

Then, the service provider management unit 390 encrypts the certificate data  $CER_{SP}$  and the signature data  $SIG_{61,ESC}$  thereof by using the session key data  $K_{SES}$   
25    obtained by the mutual certification between the mutual

certification unit 150 and the mutual certification unit 352 shown in Fig. 63 and then transmits the same to the service provider 310.

Note that, the processing where the EMD service center 302 receives the issuance request of the certificate data from the SAMs 105<sub>1</sub> to 105<sub>4</sub> is similar to the first embodiment.

Further, also the processing where the EMD service center 302 receives the registration request of the usage control policy data 106 and the content key data Kc from the content provider 301 is similar to that of the first embodiment.

Further, also the processing of preparing the key file KF in accordance with the registration use module Mod<sub>2</sub> received from the content provider 301 by the EMD service center 302 and transmitting the same to the content provider 301 is similar to the first embodiment.

Next, an explanation will be made of the processing where the EMD service center 302 receives the registration request of the price tag data 312 from the service provider 310 by referring to Fig. 70.

In this case, when the service provider management unit 390 receives the price tag registration request module Mod<sub>102</sub> shown in Fig. 69 from the service provider 310, it decrypts the price tag registration request

module  $\text{Mod}_{102}$  by using the session key data  $K_{\text{SES}}$  obtained by the mutual certification between the mutual certification unit 150 and the mutual certification unit 352 shown in Fig. 63.

5        Then, after confirming the legitimacy of the signature data  $\text{SIG}_{80, \text{SP}}$  stored in the related decrypted price tag registration request module  $\text{Mod}_{102}$  in the signature processing unit 443, the price tag data 312 stored in the price tag registration request module  $\text{Mod}_{102}$   
10    is registered and authenticated in the CER database 445a via the certificate and usage control policy management unit 445.

Next, an explanation will be made of the processing where the settlement is carried out in the EMD service  
15    center 302 by referring to Fig. 72.

When receiving as its inputs the usage log data 308 and signature data  $\text{SIG}_{205, \text{SAM1}}$  thereof from for example the SAM 305<sub>1</sub> of the user home network 303, the SAM management unit 149 decrypts the usage log data 308 and the  
20    signature data  $\text{SIG}_{205, \text{SAM1}}$  by using the session key data  $K_{\text{SES}}$  obtained by the mutual certification between the mutual certification unit 150 and the SAMs 305<sub>1</sub> to 305<sub>4</sub>, verifies the signature data  $\text{SIG}_{205, \text{SAM1}}$  by using the public key data  $K_{\text{SAM1}, \text{P}}$  of the SAM 305<sub>1</sub>, and then outputs the same  
25    to the settlement processing unit 442.

Then, the settlement processing unit 442 performs the settlement processing based on the usage log data 308 input from the SAM 305, and the suggested retailer's price data SRP and the price tag data 312 input from the certificate and usage control policy management unit 445.

The settlement processing unit 442 produces settlement report data 307c and settlement claim data 152c for the content provider 301 and outputs them to the content provider management unit 148 and the settlement manager management unit 144 as shown in Fig. 72.

Also, by the settlement processing, as shown in Fig. 70 and Fig. 72, the settlement report data 307s and the settlement claim data 152s for the service provider 310 are produced and are output to the service provider management unit 390 and the settlement manager management unit 144.

Next, the settlement manager management unit 144 performs the mutual certification of the settlement claim data 152c and 152s and the signature data produced for them by using the secret key data  $K_{ESC,S}$  and the decryption by the session key data  $K_{SES}$  and then transmits the same to the settlement manager 91 via the payment gateway 90 shown in Fig. 59.

By this, the money of the sum indicated in the settlement claim data 152c is paid to the content

provider 301, and the money of the sum indicated in the settlement claim data 152s is paid to the service provider 310.

Next, an explanation will be made of the processing  
5 in the case where the EMD service center 302 transmits the settlement report data 307c and 307s to the content provider 301 and the service provider 310.

When settlement is carried out in the settlement processing unit 442, the settlement report data 307c is  
10 output from the settlement processing unit 442 to the content provider management unit 148.

When receiving as input the settlement report data 307c from the settlement processing unit 442, the content provider management unit 148 encrypts this by using the  
15 session key data  $K_{SES}$  obtained by the mutual certification between the mutual certification unit 150 and the mutual certification unit 120 shown in Fig. 60 and then transmits the same to the content provider 301.

Also, when the settlement is carried out in the  
20 settlement processing unit 442, the settlement report data 307s is output from the settlement processing unit 442 to the service provider management unit 390.

When receiving as input the settlement report data 307s from the settlement processing unit 442, the service  
25 provider management unit 390 encrypts this by using the

session key data  $K_{SES}$  obtained by the mutual certification between the mutual certification unit 150 and the mutual certification unit 352 shown in Fig. 63 and then transmits the same to the service provider 310.

5        The EMD service center 302 performs processing at the time of shipment of the SAMs 305<sub>1</sub> to 305<sub>4</sub> and the registration processing of the SAM registration list in the same way as the EMD service center 102 of the first embodiment other than the above.

10        [User home network 303]

The user home network 303 has the network apparatus 360<sub>1</sub> and the A/V apparatuses 360<sub>2</sub> to 360<sub>4</sub> as shown in Fig. 59.

15        The network apparatus 360<sub>1</sub> includes the built-in CA module 311 and the SAM 305<sub>1</sub>. Further, the A/V apparatuses 360<sub>2</sub> to 360<sub>4</sub> include the built-in SAMs 305<sub>2</sub> to 305<sub>4</sub>.

The SAMs 305<sub>2</sub> to 305<sub>4</sub> are connected to each other via a bus 191, for example, an IEEE serial interface bus.

20        Note that, it is possible if the AV apparatuses 360<sub>2</sub> to 360<sub>4</sub> have a network communication function or do not have the network communication function, but utilize the network communication function of the network apparatus 360<sub>1</sub> via the bus 191.

Also, it is also possible if the user home network  
25    303 has only AV apparatuses not having network functions.

Below, an explanation will be made of the network apparatus 360<sub>1</sub>.

Figure 74 is a view of the configuration of the network apparatus 360<sub>1</sub>.

5       As shown in Fig. 74, the network apparatus 360<sub>1</sub> has a communication module 162, CA module 311, decryption module 905, SAM 305<sub>1</sub>, decryption and/or expansion module 163, purchase and/or usage form determination operation unit 165, download memory 167, reproduction module 169,  
10      and external memory 201.

In Fig. 74, components given the same reference numerals as those of Fig. 25 are the same as the components of the same reference numerals explained in the first embodiment.

15       The communication module 162 performs the communication processing with the service provider 310.

Concretely, the communication module 162 outputs the secure container 304 received from the service provider 310 by a satellite broadcast or the like to the  
20      decryption module 905. Also, the communication module 162 outputs user preference filter data 900 received via a telephone line or the like at the service provider 310 to the CA module 311 and, at the same time, transmits SP use purchase log data 309 input from the CA module 311 to the  
25      service provider 310 via the telephone line or the like.

Figure 75 is a functional block diagram of the CA module 311 and the decryption module 905.

As shown in Fig. 75, the CA module 311 has a mutual certification unit 906, a storage unit 907, an encryption and/or decryption unit 908 and an SP use purchase log data generation unit 909.

When transmitting and receiving the data between the CA module 311 and the service provider 310 via the telephone line, the mutual certification unit 906 performs the mutual certification with the service provider 310 to produce the session key data  $K_{SES}$  and outputs this to the encryption and/or decryption unit 908.

The storage unit 907 stores the master key data  $K_M$  supplied from the service provider 310 off-line by using an IC card 912 etc. after for example a contract is established between the service provider 310 and the user.

The encryption and/or decryption unit 908 receives as its inputs the encrypted scramble key data  $K_{SCR}$  and work key data  $K_W$  from a decryption unit 910 of the decryption module 905 and decrypts the work key data  $K_W$  by using the master key data  $K_M$  read out from the storage unit 907. Then, the encryption and/or decryption unit 908 decrypts the scramble key data  $K_{SCR}$  by using the related



decrypted work key data  $K_w$  and outputs the related  
decrypted scramble key data  $K_{scr}$  to the decryption unit  
910.

Also, the encryption and/or decryption unit 908  
5 decrypts the user preference filter data 900 received by  
the communication module 162 from the service provider  
310 via the telephone line or the like by using the  
session key data  $K_{ses}$  from the mutual certification unit  
906 and outputs the same to a secure container selection  
10 unit 911 of the decryption module 905.

Also, the encryption and/or decryption unit 908  
decrypts the SP use purchase log data 309 input from the  
SP use purchase log data generation unit 909 by using the  
session key data  $K_{ses}$  from the mutual certification unit  
15 906 and transmits the same via the communication module  
162 to the service provider 310.

The SP use purchase log data generation unit 909  
produces the SP use purchase log data 309 indicating the  
purchase log of the content data C inherent in the  
20 service provider 310 based on the operation signal S165  
in accordance with the purchase operation of the content  
data C by the user by using the purchase and/or usage  
form determination operation unit 165 shown in Fig. 74,  
or the usage control status data 166 from the SAM 305<sub>1</sub>  
25 and outputs this to the encryption and/or decryption unit

908.

The SP use purchase log data 309 includes for example the information to be collected from the user concerning the distribution service by the service  
5 provider 310, the monthly base fee (network rent), contract (update) information, and the purchase log information.

Note that, the CA module 311 communicates with a charge database, a customer management database, and a  
10 marketing information database of the service provider 310 when the service provider 310 has the charge function. In this case, the CA module 311 transmits the charge data for the distribution service of the content data to the service provider 310.

15 The decryption module 905 has a decryption unit 910 and a secure container selection unit 911.

The decryption unit 910 receives as its inputs the encrypted secure container 304, scramble key data  $K_{SCR}$ , and the work key data  $K_w$  from the communication module  
20 162.

Then, the decryption unit 910 outputs the encrypted scramble key data  $K_{SCR}$  and work key data  $K_w$  to the encryption and/or decryption unit 908 of the CA module 311 and receives as its input the decrypted scramble key  
25 data  $K_{SCR}$  from the encryption and/or decryption unit 908.

Then, the decryption unit 910 decrypts the encrypted secure container 304 by using the scramble key data  $K_{SCR}$  and then outputs the same to the secure container selection unit 911.

5        Note that, where the secure container 304 is transmitted from the service provider 310 by an MPEG2 Transport Stream method, for example, the decryption unit 910 extracts the scramble key data  $K_{SCR}$  from an ECM (Entitlement Control Message) in a TS Packet and extracts  
10      the work key data  $K_w$  from an EMM (Entitlement Management Message) .

         In the ECM, other than the above, for example, program attribute information for every channel are contained. Further, in the EMM, other than this,  
15      individual demo contract information different for every user (listener) etc. are contained.

         The secure container selection unit 911 filters the secure containers 304 input from the decryption unit 910 by using the user preference filter data 900 input from  
20      the CA module 311, selects the secure container 304 in accordance with the preference of the user, and outputs the same to the SAM 305<sub>1</sub>.

         Next, an explanation will be made of the SAM 305<sub>1</sub>.

         Note that, the SAM 305<sub>1</sub> has basically the same  
25      function and structure as the SAM 105<sub>1</sub> of the first

embodiment mentioned before by using Fig. 26 to Fig. 41 except it performs the processing concerning the service provider 310 in addition to the content provider 310, for example, it performs the signature verification processing for the service provider 310.

Also, the SAMs 305<sub>2</sub> to 305<sub>4</sub> basically have the same functions as that of the SAM 305<sub>1</sub>.

Namely, the SAMs 305<sub>1</sub> to 305<sub>4</sub> are modules for performing charge processing in units of content and communicate with the EMD service center 302.

Below, the function of the SAM 305<sub>1</sub> will be explained in detail.

Figure 76 is a view of the configuration of the SAM 305<sub>1</sub>.

Note that, in Fig. 76, the flow of the data related to the processing when receiving as input the secure container 304 from the service provider 310 is shown.

As shown in Fig. 76, the SAM 305<sub>1</sub> has the mutual certification unit 170, encryption and/or decryption units 171, 172, and 173, error correction unit 181, download memory management unit 182, secure container decryption unit 183, decryption and/or expansion module management unit 184, EMD service center management unit 185, usage monitor unit 186, signature processing unit 189, SAM management unit 190, storage unit 192, media SAM

management unit 197, stack memory 200, a service provider management unit 580, a charge processing unit 587, a signature processing unit 598, and the external memory management unit 811.

5        Note that, the predetermined function of the SAM 305<sub>1</sub> shown in Fig. 76 is realized by executing a secret program in the CPU in the same way as the case of the SAM 105<sub>1</sub>.

10        In Fig. 76, functional blocks given the same reference numerals as those of Fig. 26 are the same as the functional blocks having the same reference numerals explained in the first embodiment.

15        Also, in the external memory 201 shown in Fig. 74, after the processing explained in the first embodiment and the processing mentioned later, the usage log data 308 and the SAM registration list are stored.

20        Also, in the stack memory 200, as shown in Fig. 77, the content key data K<sub>c</sub>, usage control policy data (UCP) 106, lock key data K<sub>LOC</sub> of the storage unit 192, certificate data CER<sub>CP</sub> of the content provider 301, certificate data CER<sub>SP</sub> of the service provider 310, usage control status data (UCS) 366, SAM program download containers SDC<sub>1</sub> to SFDC<sub>3</sub>, the price tag data 312, etc. are stored.

25        Below, an explanation will be made of the functional

blocks newly given reference numerals in Fig. 76 among the functional blocks of the SAM 305<sub>1</sub>.

The signature processing unit 589 verifies the signature data in the secure container 304 by using the  
5 public key data  $K_{ESC,P}$  of the EMD service center 302, public key data  $K_{CP,P}$  of the content provider 301, and the public key data  $K_{SP,P}$  of the service provider 310 read out from the storage unit 192 or the stack memory 200.

The charge processing unit 587 performs the charge  
10 processing in accordance with the purchase and/or usage form of the content by the user based on the operation signal S165 from the purchase and/or usage form determination operation unit 165 shown in Fig. 74 and the price tag data 312 read out from the stack memory 200 as  
15 shown in Fig. 78.

The charge processing by the charge processing unit 587 is carried out based on the rights contents such as the usage permission condition indicated by the usage control policy data 106 and the usage control status data  
20 166 under the monitoring of the usage monitor unit 186. Namely, the user can purchase and use the content within the range according to the related rights content etc.

Also, the charge processing unit 587 produces the usage log data 308 in the charge processing and writes  
25 this into the external memory 201 via the external memory

management unit 811.

Here, the usage log data 308 is used when determining the payment of the license fee related to the secure container 304 in the EMD service center 302 in the same way as the usage log data 108 of the first embodiment.

Also, the charge processing unit 587 produces the usage control status (UCS) data 166 describing the purchase and/or usage form of the content by the user based on the operation signal S165 and writes this into the stack memory 200.

As the purchase form of the content, there are for example outright purchase without restriction as to the reproduction by the purchaser or copying for use of the related purchaser and a reproduction charge for charging whenever the content is reproduced.

Here, the usage control status data 166 is produced when the user determines the purchase form of the content and used for control so that the user will use the related content within the range permitted by the related determined purchase form from then on. In the usage control status data 166, the ID of the content, purchase form, outright purchase price, SAM\_ID of the SAM for which the related content was purchased, the USER\_ID of the user purchasing the content, etc. are described.

Note that, where the determined purchase form is a reproduction charge, for example, the usage control status data 166 is transmitted from the SAM 305<sub>1</sub> to the service provider 310 in real-time, and the service  
5 provider 310 instructs the EMD service center 302 to take the usage log data 308 from the SAM 105<sub>1</sub>.

Also, where the determined purchase form is outright purchase, for example, the usage control status data 166 is transmitted to the service provider 310 and the EMD  
10 service center 302 in real-time.

Also, in the SAM 305<sub>1</sub>, as shown in Fig. 76, the user preference filter data 903 received via the EMD service center management unit 185 from the EMD service center 302 is output to the service provider management unit  
15 580. Then, in the service provider management unit 580, among the secure containers 304 input from the decryption module 905 shown in Fig. 74, the secure container 304 filtered based on the user preference filter data 903 and thus responding to the preference of the user is  
20 selected, and the related selected secure container 304 is output to the error correction unit 181. By this, in the SAM 305<sub>1</sub>, the selection processing of the content data C based on the preference of the related user obtained from the purchase situation of the content data  
25 C by the related user becomes possible for all service



providers 310 contracting with the user of the related SAM 305<sub>1</sub>.

Below, the flow of the processing in the SAM 305<sub>1</sub> will be explained.

5       The flow of the processing when storing the distribution use key data KD<sub>1</sub> to KD<sub>3</sub> received from the EMD service center 302 in the storage unit 192 is similar to that of the case of the SAM 105<sub>1</sub> mentioned before.

Next, an explanation will be made of the flow of the  
10       processing in the SAM 305<sub>1</sub> when receiving as input the secure container 304 from the service provider 310 by referring to Fig. 76.

Mutual certification is carried out between the mutual certification unit 170 and the mutual  
15       certification unit 352 of the service provider 310 shown in Fig. 63.

The encryption and/or decryption unit 171 decrypts the secure container 304 shown in Fig. 65 received from the service provider 310 via the service provider  
20       management unit 580 by using the session key data K<sub>SES</sub> obtained by the related mutual certification.

Next, the signature processing unit 589 verifies the signature data SIG<sub>61,ESC</sub> and SIG<sub>1,ESC</sub> shown in Fig. 65D, and then verifies the legitimacy of the signature data  
25       SIG<sub>6,CP</sub>, SIG<sub>62,SP</sub>, SIG<sub>7,CP</sub>, SIG<sub>63,SP</sub>, and SIG<sub>64,SP</sub> by using the

public key data  $K_{SP,P}$  and  $K_{CP,P}$  stored in the certificate data  $CER_{SP}$  and  $CER_{CP}$ .

Here, by verifying the signature data  $SIG_{6,CP}$  and  $SIG_{62,SP}$ , the legitimacy of the producer and transmitter of the content file CF is confirmed, by verifying the signature data  $SIG_{7,CP}$  and  $SIG_{63,SP}$ , the legitimacy of the transmitter of the key file KF is confirmed, and by verifying the signature data  $SIG_{64,SP}$ , the legitimacy of the producer and the transmitter of the price tag data 312 is confirmed.

Also, by verifying the legitimacy of the signature data  $SIG_{K1,ESC}$  stored in the key file KF shown in Fig. 65B by using the public key data  $K_{ESC,P}$  read out from the storage unit 192, the signature processing unit 589 verifies the legitimacy of the producer of the key file KF and whether or not the key file KF is registered in the EMD service center 302.

When the legitimacy of all signature data mentioned above is confirmed in the signature processing unit 589, the service provider management unit 580 outputs the secure container 304 to the error correction unit 181.

The error correction unit 181 corrects the error of the secure container 304 and then outputs the same to the download memory management unit 182.

The download memory management unit 182 performs the

mutual certification between the mutual certification unit 170 and the media SAM 167a shown in Fig. 74 and then writes the secure container 304 into the download memory 167.

5       Next, the download memory management unit 182 performs the mutual certification between the mutual certification unit 170 and the media SAM 167a shown in Fig. 74 and then reads out the key file KF shown in Fig. 65B stored in the secure container 304 from the download  
10       memory 167 and outputs the same to the secure container decryption unit 183.

Then, in the secure container decryption unit 183, by using the distribution use data  $KD_1$  to  $KD_3$  of the corresponding period input from the storage unit 192, the  
15       content key data  $Kc$ , usage control policy data 106, and the SAM program download containers  $SDC_1$  to  $SDC_3$  stored in the key file KF shown in Fig. 65B are decrypted.

Then, the decrypted content key data  $Kc$ , usage control policy data 106, and the SAM program download  
20       containers  $SDC_1$  to  $SDC_3$  are written into the stack memory 200.

Below, an explanation will be made of the flow of the processing until the purchase form of the secure container 304 downloaded on the download memory 167 from  
25       the service provider 310 is determined by referring to

Fig. 78 and Fig. 79.

Figure 79 is a flowchart for explaining the purchase form determination processing of the secure container 304.

5           <Step E1>

Where the operation signal S165 indicating the demo mode is output to the charge processing unit 587 by the operation of the purchase and/or usage form determination operation unit 165 shown in Fig. 74 by the user, the  
10       processing of step E2 is carried out. In other cases, the processing of step E3 is carried out.

          <Step E2>

This is carried out where the operation signal S165 indicating the demo mode is output to the charge  
15       processing unit 587, and for example the content file CF stored in the download memory 167 is output via the decryption and/or expansion module management unit 184 to the decryption and/or expansion module 163 shown in Fig.  
74.

20           At this time, with respect to the content file CF, the mutual certification between the mutual certification unit 170 and the media SAM 167a and the encryption and/or decryption by the session key data  $K_{SES}$  and the mutual  
certification between the mutual certification unit 170  
25       and the mutual certification unit 220 and the encryption

and/or decryption by the session key data  $K_{SES}$  are carried out.

The content file CF is decrypted in the decryption unit 221 shown in Fig. 74 by using the session key data  $K_{SES}$  and then output to the decryption unit 222.

Also, the content key data Kc and the half disclosure parameter data 199 read out from the stack memory 200 are output to the decryption and/or expansion module 163 shown in Fig. 74. At this time, after the mutual certification between the mutual certification unit 170 and the mutual certification unit 220, the encryption and decryption by the session key data  $K_{SES}$  are carried out with respect to the content key data Kc and the half disclosure parameter data 199.

Next, the decrypted half disclosure parameter data 199 is output to the half disclosure processing unit 225, and under the control from the half disclosure processing unit 225, the decryption of the content data C using the content key data Kc by the decryption unit 222 is carried out in a half disclosure mode.

Next, the content data C decrypted in the half disclosure mode is expanded at the expansion unit 223 and then output to the electronic watermark information processing unit 224.

Next, the user watermark use data 196 is buried in

the content data C in the electronic watermark information processing unit 224, then the content data C is reproduced at the reproduction module 169, and sound in accordance with the content data C is output.

5           <Step E3>

When the user determines the purchase form by operating the purchase and/or usage form determination operation unit 165, the operation signal S165 indicating the related determined purchase form is output to the charge processing unit 187.

          <Step E4>

In the charge processing unit 187, the usage log data 308 and the usage control status data 166 in accordance with the determined purchase form are produced, the usage log data 308 is written into the external memory 201 via the external memory management unit 811, and the usage control status data 166 is written into the stack memory 200.

Thereafter, in the usage monitor unit 186, control (monitor) is carried out so that the content is purchased and used within the range permitted by the usage control status data 166.

Then, by using the key file KF and the usage control status data 166 stored in the stack memory 200, a new key file KF<sub>1</sub> with the purchase form determined therefor shown

in Fig. 81C is produced, and the related produced key file  $KF_1$  is stored in the stack memory 200.

As shown in Fig. 81C, the usage control status data 166 stored in the key file  $KF_1$  has been sequentially  
5 encrypted by utilizing the CBC mode of the DES by using the storage key data  $K_{STR}$  and the media key data  $K_{MED}$ .

Here, the storage use key data  $K_{STR}$  is data determined in accordance with the type of apparatus, for example, an SACD (Super Audio Compact Disc), DVD (Digital  
10 Versatile Disc) apparatus, CD-R apparatus, and MD (Mini Disc) apparatus, and used for establishing one-to-one correspondence between the types of the apparatuses and the types of the storage medium. Also, the media key data  $K_{MED}$  is data unique to the storage medium.

15 Also, in the signature processing unit 589, the hash value  $H_{K1}$  of the key file  $KF_1$  is produced by using the secret key data  $K_{SAM1,S}$  of the SAM 305<sub>1</sub>, and the related produced hash value  $H_{K1}$  is stored in the stack memory 200 in correspondence to the key file  $KF_1$ .

20 <Step E5>

The usage control status data 166 is transmitted from the SAM 305<sub>1</sub> to the EMD service center 302. The related usage control status data 166 is transmitted whenever the purchase form of the content data is  
25 determined in the SAM 305.

Note that, the usage log data 308 is transmitted from the SAM 305<sub>1</sub> to the EMD service center 302 at predetermined time intervals of for example one month.

Next, an explanation will be made of the flow of the  
5 processing in the case where the content data C for which the purchase form is already determined stored in the download memory 167 is reproduced by referring to Fig. 78.

In this case, under the monitoring by the usage  
10 monitor unit 186, based on the operation signal S165, the content file CF stored in the download memory 167 is output to the decryption and/or expansion module 163 shown in Fig. 74.

Also, the content key data Kc read out from the  
15 stack memory 200 is output to the decryption and/or expansion module 163.

Then, in the decryption unit 222 of the decryption  
and/or expansion module 163, the decryption of the  
content file CF using the content key data Kc and the  
20 expansion processing by the expansion unit 223 are carried out, and the content data C is reproduced in the reproduction module 169.

At this time, in the charge processing unit 587, the  
usage log data 308 stored in the external memory 201 is  
25 updated in response to the operation signal S165.



The usage log data 308 is transmitted together with the signature data  $SIG_{205, SAM1}$  produced by using the secret key data  $K_{SAM1, S}$  via the EMD service center management unit 185 to the EMD service center 302 at a predetermined timing.

Next, as shown in Fig. 80, an explanation will be made of the flow of the processing in the SAM 305<sub>1</sub> in the case where, for example, the secure container 304x shown in Fig. 81 for which the purchase form has been already determined and downloaded on the download memory 167 of the network apparatus 360<sub>1</sub> is transferred via the bus 191 to the SAM 305<sub>1</sub> of the AV apparatus 360<sub>2</sub> by referring to Fig. 82.

The user operates the purchase and/or usage form determination operation unit 165 to instruct to transfer the predetermined content stored in the download memory 167 to the AV apparatus 360<sub>2</sub>. The operation signal S165 in accordance with the related operation is output to the charge processing unit 587.

By this, the charge processing unit 587 updates the usage log data 308 stored in the stack memory 200 based on the operation signal S165.

Also, the download memory management unit 182 outputs the content files CF and key files KF and KF<sub>1</sub> shown in Figs. 81A, 81B and 81C read out from the

download memory 167 to the signature processing unit 589 and the SAM management unit 190.

Then, the signature processing unit 589 produces the signature data  $SIG_{41, SAM1}$  and  $SIG_{42, SAM1}$  of the content files CF and the key files KF and, at the same time, produces the hash value  $H_{K1}$  of the key file  $KF_1$ , and outputs them to the SAM management unit 190.

Also, the SAM management unit 190 reads out the price tag data 312 and the signature data  $SIG_{64, SP}$  thereof and the certificate data  $CER_{CP}$  and the signature data  $SIG_{1, ESC}$  thereof shown in Figs. 81D and 81E from the stack memory 200.

Also, the SAM management unit 190 reads out the certificate data  $CER_{SAM1}$  and the signature data  $SIG_{22, ESC}$  thereof shown in Fig. 81E from the storage unit 192.

Next, the SAM management unit 190 produces the secure container 304x shown in Fig. 81.

Also, the mutual certification unit 170 outputs the session key data  $K_{SES}$  obtained by mutual certification with the SAM 305<sub>2</sub> to the encryption and/or decryption unit 171.

The SAM management unit 190 encrypts the secure container 304x shown in Fig. 81 in the encryption and/or decryption unit 171 by using the session key data  $K_{SES}$  and then outputs the same to the SAM 305<sub>2</sub> of the AV apparatus

360<sub>2</sub> shown in Fig. 82.

Below, as shown in Fig. 80, an explanation will be made of the flow of the processing in the SAM 305<sub>2</sub> when writing the secure container 304x input from the SAM 305<sub>1</sub> into a storage medium such as a RAM by referring to Fig. 83.

In this case, the SAM management unit 190 of the SAM 305<sub>2</sub> receives as input the secure container 304x shown in Fig. 81 from the SAM 305<sub>1</sub> of the network apparatus 360<sub>1</sub> as shown in Fig. 83.

Then, the mutual certification between the mutual certification unit 170 of the SAM 305<sub>1</sub> and the mutual certification unit 170 of the SAM 305<sub>2</sub> is carried out, and the signature processing unit 589 decrypts the secure container 304x by using the session key data  $K_{SES}$  obtained by the related mutual certification.

Next, in the signature processing unit 589, by using the public key data  $K_{ESC,P}$  read out from the storage unit 192, the legitimacy of the signature data  $SIG_{61,ESC}$ ,  $SIG_{1,ESC}$ , and  $SIG_{22,ESC}$  shown in Fig. 81E is verified.

Then, when the legitimacy of the signature data  $SIG_{61,ESC}$ ,  $SIG_{1,ESC}$ , and  $SIG_{22,ESC}$  is confirmed, in the signature processing unit 589, by using the public key data  $K_{SP,P}$ ,  $K_{CP,P}$ , and  $K_{SAM1,P}$  contained in the certificate data  $CER_{SP}$ ,  $CER_{CP}$ , and  $CER_{SAM1}$ , the legitimacy of the

signature data  $SIG_{6,CP}$ ,  $SIG_{62,SP}$ ,  $SIG_{41,SAM1}$ ,  $SIG_{7,CP}$ ,  $SIG_{63,SP}$ ,  
 $SIG_{42,SAM1}$ , and  $SIG_{64,SP}$  shown in Figs. 81A to 81D and the  
hash value  $H_{K1}$  is verified.

Then, when the legitimacy of these signature data is  
5 confirmed, the key files  $KF$  and  $KF_1$  and the price tag  
data 312 are stored in the stack memory 200.

Also, the content file  $CF$  is output from the  $SAM$   
management unit 190 to the storage module management unit  
855.

10 Then, the content key data  $Kc$  and the usage control  
status data 166 stored in the key file  $KF_1$  shown in Fig.  
81C are read out from the stack memory 200 to the  
encryption and/or decryption unit 173, and in the  
encryption and/or decryption unit 173, sequentially  
15 encrypted by using the storage use key distribution use  
data  $KD_{STR}$ , media key data  $K_{MED}$ , and the purchaser key data  
 $K_{PIN}$  read out from the storage unit 192 and then output to  
the storage module management unit 855.

Also, the key file  $KF$  read out from the stack memory  
20 200 is output to the storage module management unit 855.

Then, after the mutual certification between the  
mutual certification unit 170 and the media  $SAM$  133 of  
the RAM type storage medium 130<sub>4</sub>, the content file  $CF$  is  
stored in the unsecure RAM region 134 of the RAM type  
25 storage medium 130<sub>4</sub>, and the key files  $KF$  and  $KF_1$  and the

price tag data 312 are written into the secure RAM region 132.

Note that, it is also possible to store the key files KF and KF<sub>1</sub> and the price tag data 312 in the media SAM 133 of the RAM type storage medium 130<sub>4</sub>.

Note that, among the processing in the SAM 305<sub>1</sub>, the flow of the processing in the AV apparatus 360<sub>2</sub> when determining the purchase form of the ROM type storage medium with the purchase form of the content still undetermined and the flow of the processing when reading the secure container 304 from the ROM type storage medium with the purchase form still undetermined in the AV apparatus 360<sub>3</sub>, transferring this to the AV apparatus 360<sub>2</sub>, and writing the same into the RAM type storage medium are the same as the case of the SAM 105<sub>1</sub> of the first embodiment except for the point that the signature data is verified using the secret key data of the service provider 310 and for the point that the price tag data 312 is stored in the key file with the purchase form determined.

Next, an explanation will be made of the overall operation of the EMD system 300 shown in Fig. 59.

Figure 84 and Fig. 85 are flowcharts of the overall operation of the EMD system 300.

Here, an explanation will be made by exemplifying

the case where the secure container 304 is transmitted from the service provider 310 to the user home network 303 on-line.

Note that, as the prerequisite of the following processing, it is assumed that the registration of the content provider 301, service provider 310, and SAMs 305<sub>1</sub> to 305<sub>4</sub> to the EMD service center 302 has been already finished.

Step S21: The EMD service center 302 transmits the certificate  $CER_{CP}$  of the public key data  $K_{CP,P}$  of the content provider 301 together with the its own signature data  $SIG_{1,ESC}$  to the content provider 301.

Also, the EMD service center 302 transmits the certificate  $CER_{SP}$  of the public key data  $K_{SP,P}$  of the content provider 301 together with its own signature data  $SIG_{61,ESC}$  to the service provider 310.

Also, the EMD service center 302 transmits three months' worth of the distribution use key data  $KD_1$  to  $KD_3$  each having the expiration date of one month to the SAMs 305<sub>1</sub> to 305<sub>4</sub> of the user home network 303.

Step S22: After the mutual certification, the content provider 301 transmits the registration use module  $Mod_2$  shown in Fig. 18 to the EMD service center 302.

Then, after the predetermined signature

verification, the EMD service center 302 registers and authenticates the usage control policy data 106 and content key data Kc.

Also, the EMD service center 302 produces six  
5 months' worth of the key files KF shown in Fig. 5B in accordance with the registration use module Mod<sub>2</sub>, and transmits this to the content provider 301.

Step S23: The content provider 301 produces the content file CF and the signature data SIG<sub>6,CP</sub> thereof and  
10 the key file KF and the signature data SIG<sub>7,CP</sub> thereof shown in Figs. 5A and 5B and provides the secure container 104 storing them and the certificate data CER<sub>CP</sub> and the signature data SIG<sub>1,ESC</sub> thereof shown in Fig. 5C to the service provider 310 on-line and/or off-line.

15 Step S24: The service provider 310 verifies the signature data SIG<sub>1,ESC</sub> shown in Fig. 5C and then verifies the signature data SIG<sub>6,CP</sub> and SIG<sub>7,CP</sub> shown in Figs. 5A and 5B by using the public key data K<sub>CP,P</sub> stored in the certificate data CER<sub>CP</sub> and confirms if the secure  
20 container 104 was transmitted from a legitimate content provider 301.

Step S25: The service provider 310 produces the price tag data 312 and the signature data SIG<sub>64,SP</sub> thereof and produces the secure container 304 shown in Fig. 65  
25 storing them.

Step S26: The service provider 310 transmits the price tag registration request module  $\text{Mod}_{102}$  shown in Fig. 69 to the EMD service center 302.

Then, the EMD service center 302 registers and  
5 authenticates the price tag data 312 after the predetermined signature verification.

Step S27: The service provider 310 transmits the secure container 304 produced at step S25 on-line or off-line to the decryption module 905 of the network  
10 apparatus  $360_1$  shown in Fig. 74 in response to the request from for example the CA module 311 of the user home network 303.

Step S28: The CA module 311 produces the SP use purchase log data 309 and transmits this to the service  
15 provider 310 at the predetermined timing.

Step S29: In any of the SAMs  $305_1$  to  $305_4$ , after verifying the signature data  $\text{SIG}_{61, \text{ESC}}$  shown in Fig. 65D, the signature data  $\text{SIG}_{62, \text{SP}}$ ,  $\text{SIG}_{63, \text{SP}}$ , and  $\text{SIG}_{64, \text{SP}}$  shown in Figs. 65A, 65B and 65C are verified by using the public  
20 key data  $K_{\text{SP}, \text{P}}$  stored in the certificate data  $\text{CER}_{\text{SP}}$ , and it is confirmed whether or not the predetermined data in the secure container 304 was produced and transmitted in a legitimate service provider 310.

Step S30: After verifying the signature data  $\text{SIG}_{1, \text{ESC}}$   
25 shown in Fig. 65D in any of the SAMs  $305_1$  to  $305_4$ , the



signature data  $SIG_{6,SP}$  and  $SIG_{7,SP}$  shown in Figs 65A, 65B and 65C are verified by using the public key data  $K_{CP,P}$  stored in the certificate data  $CER_{CP}$ , and it is confirmed whether or not the content file CF in the secure

5 container 304 was produced in a legitimate content provider 301 and whether or not the key file KF was transmitted from a legitimate content provider 301.

Also, by verifying the legitimacy of the signature data  $SIG_{K1,ESC}$  in the key file KF shown in Fig. 65B by  
10 using the public key data  $K_{ESC,P}$  in any of the SAMs 305<sub>1</sub> to 305<sub>4</sub>, it is confirmed whether or not the key file KF was produced by a legitimate EMD service center 302.

Step S31: The user operates the purchase and/or usage form determination operation unit 165 of Fig. 74  
15 and determines the purchase and/or usage form of the content.

Step S32: Based on the operation signal S165 produced at step S31, in the SAMs 305<sub>1</sub> to 305<sub>4</sub>, the usage log data 308 of the secure container 304 is produced.

20 The usage log data 308 and the signature data  $SIG_{205,SAM1}$  thereof are transmitted from the SAMs 305<sub>1</sub> to 305<sub>4</sub> to the EMD service center 302.

Also, whenever the purchase form is determined, the usage control status data 166 is transmitted from the  
25 SAMs 305<sub>1</sub> to 305<sub>4</sub> to the EMD service center 302.

Step S33: The EMD service center 302 determines (calculates) the charge content for each of the content provider 301 and the service provider 310 based on the usage log data 308 and produces the settlement claim data 152c and 152s based on the result thereof.

Step S34: The EMD service center 302 transmits the settlement claim data 152c and 152s together with its own signature data to the settlement manager 91 via the payment gateway 90. By this, the money paid by the user of the user home network 303 to the settlement manager 91 is distributed to the owners of the content provider 301 and the service provider 310.

As explained above, in the EMD system 300, the secure container 104 of the format shown in Fig. 5 is distributed from the content provider 301 to the service provider 310, the secure container 304 storing the content file CF and key file KF in the secure container 104 as they are is distributed from the service provider 310 to the user home network 303, and the processing for the key file KF is carried out in the SAMs 305<sub>1</sub> to 305<sub>4</sub>.

Also, the content key data Kc and usage control policy data 106 stored in the key file KF have been encrypted by using the distribution use key data KD<sub>1</sub> to KD<sub>3</sub> and decrypted in only the SAMs 305<sub>1</sub> to 305<sub>4</sub> holding the distribution use key data KD<sub>1</sub> to KD<sub>3</sub>. The SAMs 305<sub>1</sub> to

305<sub>4</sub> are modules having tamper resistance. The purchase form and the usage form of the content data C are determined based on the handling content of the content data C described in the usage control policy data 106.

5       Accordingly, according to the EMD system 300, the content data C can be reliably purchased and used in the user home network 303 based on the content of the usage control policy data 106 produced by the interested party of the content provider 101 irrelevant to the processing  
10   in the service provider 310. Namely, according to the EMD system 300, it is possible to prevent the usage control policy data 106 from being managed by the service provider 310.

For this reason, according to the EMD system 300,  
15   even in a case where the content data C is distributed to the user home network 303 via a plurality of service providers 310 of different affiliations, the rights clearing for the related content data C in the user home network 303 can be performed based on the common usage  
20   control policy data 106 produced by the content provider 301.

Also, in the EMD system 300, for the files and data in the secure containers 104 and 304, the signature data indicating the legitimacy of the producers and the  
25   transmitters of them are stored. Therefore, in the

service provider 310 and the SAMs 305<sub>1</sub> to 305<sub>4</sub>, the  
legitimacy of the producers and transmitters and whether  
or not the data has been tampered with can be confirmed.  
As a result, the illegitimate usage of the content data C  
5 can be effectively avoided.

Also, in the EMD system 300, by distributing the  
content data C from the service provider 310 to the user  
home network 103 by using the secure container 304 in  
both of the cases of on-line and off-line, in both cases,  
10 common rights clearing of the content data C in the SAMs  
305<sub>1</sub> to 305<sub>4</sub> can be performed.

Also, in the EMD system 300, when purchasing, using,  
recording, and transferring the content data C in the  
network apparatus 360<sub>1</sub> and the AV apparatuses 360<sub>2</sub> to 360<sub>4</sub>,  
15 in the user home network 303, by always performing the  
processing based on the usage control policy data 106,  
common rights clearing rules can be employed.

For example, as shown in Fig. 86, no matter by what  
technique (route) the content data C provided by the  
20 content provider 301 is distributed (delivered) from the  
service provider 310 to the user home network 303, such  
as package communication, a digital broadcast, Internet,  
dedicated line, digital radio, and mobile communication,  
in the SAMs of the user home networks 303 and 303a,  
25 common rights clearing rules are employed based on the

usage control policy data 106 produced by the content provider 301.

Also, according to the EMD system 300, since the EMD service center 302 has the certificate authority  
5 function, key data management function, and the rights clearing (profit distribution) function, the money paid by the user accompanied with the usage of the content is reliably distributed to the owners of the content provider 301 and the EMD service center 302 according to  
10 the ratio determined in advance.

Also, according to the EMD system 300, the usage control policy data 106 for the same content file CF supplied by the same content provider 301 is supplied as is to the SAMs 305<sub>1</sub> to 305<sub>4</sub>, irrelevant as to the service  
15 format of the service provider 310. Accordingly, in the SAMs 305<sub>1</sub> to 305<sub>4</sub>, the content file CF can be used according to the intention of the content provider 301 based on the usage control policy data 106.

Namely, according to the EMD system 300, at the time  
20 of a service using the content and usage of the content by the user, the rights and profit of the owner of the content provider 301 can be reliably protected by technical means without depending on an inspection organization 725 as in the conventional case.

25 Below, an explanation will be made of a concrete

example of the transport protocol such as the secure container employed in the EMD system 300 of the above second embodiment.

As shown in Fig. 87, the secure container 104  
5 produced in the content provider 301 is provided to the service provider 310 by using a content provider use transport protocol of the Internet (TCP/IP) or dedicated line (ATM cell).

Also, the service provider 310 distributes the  
10 secure container 304 produced by using the secure container 104 to the user home network 303 by using the service provider use transport protocol of a digital broadcast (XML/SMIL on MPEG-TS), Internet (XML/SMIL on TCP/IP), or package circulation (storage medium).

Also, the secure container is transferred among SAMs  
15 in the user home networks 303 and 303a or between the user home network 303 and 303a by using the home EC/distribution service (XML/SMIL on 1394 serial bus . interface) or storage medium.

Below, an example of the transport protocol employed  
20 in the data transfer in the routes indicated by reference symbols A to G will be explained in detail in Fig. 87.

Figure 88 is a view for explaining the transport  
protocol employed when transporting the secure container  
25 104 etc. between the content provider 301 and the service

provider 310 (symbol A) shown in Fig. 87.

As shown in Fig. 88, the secure container 104 etc.  
are transported from the content provider 301 to the  
service provider 310 by a session using a common key in  
5 the IP/IP-SEC layer, SSL (Secure Sockets Layer), XML  
(Extensible Markup Language)/SMIL (Synchronized  
Multimedia Integration Language) layer, and application  
layer.

Figure 89 is a view for explaining the transport  
10 protocol employed when transporting the key file etc.  
between the EMD service center 302 and the content  
provider 301 (symbol B) shown in Fig. 87.

As shown in Fig. 89, the key file etc. are  
transported from the EMD service center 302 to the  
15 content provider 301 by a session using a common key in  
the IP/IP-SEC layer, SSL layer, and the application  
layer.

Figure 90 is a view for explaining the transport  
protocol employed when transporting the price tag data  
20 312 etc. between the EMD service center 302 and the  
service provider 310 (symbol C) shown in the figure.

As shown in Fig. 90, the price tag data 312 etc. are  
transported from the EMD service center 302 to the  
service provider 310 by a session using a common key in  
25 the IP/IP-SEC layer, SSL layer, and the application

layer.

Figure 91 is a view for explaining the transport protocol employed when transporting the secure container 304 etc. between the service provider 310 and the user home network 303 (symbol D) and in the user home network 303 (symbol E) shown in Fig. 87.

As shown in Fig. 91, the secure container 304 etc. are transported from the service provider 310 to the network apparatus 360<sub>1</sub> of the user home network 303.

At this time, the MPEG-TS layer, PES layer, or DSM-CC\_Data\_Carousel layer and MHEG (Multimedia and Hypermedia Experts) layer or "http layer and XML/SMIL layer" are used as the service provider use commodity transport protocol for transferring the secure container 304 between the service provider 310 and the network apparatus 360<sub>1</sub>.

Also, between the network apparatus 360<sub>1</sub> and a storage apparatus 360<sub>2</sub> and between AV apparatuses, HAVi (XML) is used as the user home network commodity transport protocol for transferring the secure container.

At this time, where XML/SMIL/BML is utilized in the data broadcast method of a digital broadcast, the content files CF1 and CF2 and the key files KF1 and KF2 and the demo sample of the secure container 304 are stored in a BML/XML/SMIL layer on the HTTP layer and a monomedia data



layer and transported as shown in Fig. 92.

Also, where the MHEG is utilized in the data broadcast method of a digital broadcast, the content files CF1 and CF2 and the key files KF1 and KF2 and the demo sample of the secure container 304 are stored in the monomedia data layer on the MHEG layer and transported as shown in Fig. 93.

Also, where the XML/SMIL is utilized in the data broadcast method of a digital broadcast, the content files CF1 and CF2 and the key files KF1 and KF2 and the demo sample of the secure container 304 are stored in the XML/SMIL layer on the HTTP layer and transported as shown in Fig. 94.

Figure 95 is a view for explaining the transport protocol employed when the usage log data 308 and the usage control status data 166 etc. are transported between the EMD service center 302 and the user home networks 303 and 303a (symbol G) shown in Fig. 87.

As shown in Fig. 95, where the usage log data 308 etc. are transferred from the network apparatus 360<sub>1</sub> to the EMD service center 302, a session using the session key data is carried out in the IP/IP-SEC layer, SSL layer, and the application layer.

Also, where the network apparatus 360<sub>2</sub> etc. transfer the usage log data 308, usage control status data 166,

etc. to the EMD service center 302, after the usage log data 308 etc. are transferred from the storage apparatus 360<sub>2</sub> to the network apparatus 360<sub>1</sub> by a session in the IP/IP-SEC layer and the HAVi layer, they are transferred  
5 from the network apparatus 360<sub>1</sub> to the EMD service center 302 as mentioned before.

Figure 96 is a view for explaining the transport protocol employed when transporting the secure container from the storage apparatus 360<sub>4</sub> of the user home network  
10 303 to the storage apparatus 360<sub>11</sub> of the user home network 303a shown in Fig. 87.

As shown in Fig. 96, the secure container is transported from the storage apparatus 360<sub>4</sub> to the storage apparatus 360<sub>11</sub> by a session using a common key  
15 in the IP/IP-SEC layer, SSL layer, XML/SMIL layer, and the application layer.

#### First modification of second embodiment

Figure 97 is a view of the configuration of an EMD system 300a using two service providers according to a  
20 first modification of the second embodiment.

In Fig. 97, components given the same reference numerals as those of Fig. 59 are the same as the components having the same reference numerals explained in the first embodiment.

25 As shown in Fig. 97, in the EMD system 300a, the

same secure containers 104 are supplied from the content provider 301 to service providers 310a and 310b.

The service provider 310a offers a service providing for example a drama program as the content. In the related service, a secure container 304a storing the content data C related to the drama program and price tag data 312a uniquely produced for the related content data C is produced and is distributed to the network apparatus 360<sub>1</sub>.

Also, the service provider 310b provides for example a karaoke service. In the related service, a secure container 304b storing the content data C related to the karaoke service and price tag data 312b uniquely produced for the related content data C is produced and is distributed to the network apparatus 360<sub>1</sub>.

Here, the formats of the secure containers 304a and 304b are the same as that of the secure container 304 explained by using Fig. 65.

A network apparatus 360a<sub>1</sub> is provided with CA modules 311a and 311b corresponding to the service providers 310a and 310b.

The CA modules 311a and 311b are receive the secure containers 304a and 304b in response to requests from them to the service providers 310a and 310b.

Next, the CA modules 311a and 311b produce SP use

purchase log data 309a and 309b in accordance with the distributed secure containers 304a and 304b and transmit them to the service providers 310a and 310b.

Also, the CA modules 311a and 311b decrypt the  
5 secure containers 304a and 304b by the session key data  $K_{SES}$  and then output the same to the SAMs 305<sub>1</sub> to 305<sub>4</sub>.

Next, in the SAMs 305<sub>1</sub> to 305<sub>4</sub>, the key files KF in the secure containers 304a and 304b are decrypted by using the common distribution use key data KD<sub>1</sub> to KD<sub>3</sub>,  
10 the processing concerning the purchase and/or usage of the content in accordance with the operation from the user is carried out based on the common usage control policy data 106, and the usage log data 308 in accordance with that is produced.

15 Then, the usage log data 308 is transmitted from the SAMs 305<sub>1</sub> to 305<sub>4</sub> to the EMD service center 302.

In the EMD service center 302, based on the usage log data 308, the charge content is determined (calculated) for each of the content provider 301 and the  
20 service providers 310a and 310b, and the settlement claim data 152c, 152sa, and 152sb corresponding to them are produced based on the results thereof.

The EMD service center 302 transmits the settlement claim data 152c, 152sa, and 152sb to the settlement  
25 manager 91 via the payment gateway 90. By this, the money

paid by the user of the user home network 303 to the settlement manager 91 is distributed to the owners of the content provider 301 and the service providers 310a and 310b.

5       As mentioned above, according to the EMD system 300a, when the same content file CF is supplied to the service providers 310a and 310b, the usage control policy data 106 for the related content file CF is encrypted by the distribution use key data  $KD_1$  to  $KD_6$  and supplied to  
10   the service providers 310a and 310b, and the service providers 310a and 310b distribute the secure containers 304a and 304b storing the encrypted usage control policy data 106 as it is to the user home network. For this reason, in the SAMs 305<sub>1</sub> to 305<sub>4</sub> in the user home  
15   network, no matter which of the service provider 310a or 310b the content file CF is distributed from, the rights can be cleared based on the common usage control policy data 106.

      Note that, in the first modification, the case where  
20   two service providers were used was exemplified, but in the present invention, any number of the service providers may be provided.

Second modification of second embodiment

      Figure 98 is a view of the configuration of an EMD  
25   system 300b using a plurality of content providers

according to a second modification of the second embodiment.

In Fig. 98, components given the same reference numerals as those of Fig. 59 are the same as the  
5 components having the same reference numerals explained in the first embodiment.

As shown in Fig. 98, in the EMD system 300b, the key files KFa and KFb are supplied from the EMD service center 302 to the content providers 301a and 301b, and  
10 the secure containers 104a and 104b are supplied from content providers 301a and 301b to the service provider 310.

The service provider 310 provides a service by using the content supplied by for example the content providers  
15 301a and 301b, produces the price tag data 312a for the secure container 104a and the price tag data 312b for the secure container 104b, and produces a secure container 304c storing them.

As shown in Fig. 98, in the secure container 304c,  
20 the content data CFa, CFb, key files KFa and KFb, price tag data 312a and 312b, and the signature data by the secret key data  $K_{CP,s}$  of the service provider 310 for each of them are stored.

The secure container 304c is received at the CA  
25 module 311 of the network apparatus 360<sub>1</sub> of the user home

network 303 and then processed at the SAMs 305<sub>1</sub> to 305<sub>4</sub>.

In the SAMs 305<sub>1</sub> to 305<sub>4</sub>, the key file KFa is  
decrypted by using the distribution use key data KDa<sub>1</sub> to  
KDa<sub>3</sub>, the processing concerning the purchase and/or usage  
5 is carried out in accordance with the operation from the  
user for the content file CFa based on the usage control  
policy data 106a, and the log thereof is described in the  
usage log data 308.

Also, in the SAMs 305<sub>1</sub> to 305<sub>4</sub>, the key file Kfb is  
10 decrypted by using distribution use key data KDb<sub>1</sub> to  
KDb<sub>3</sub>, the processing concerning the purchase and/or usage  
is carried out in accordance with the operation from the  
user for the content file CFb based on the usage control  
policy data 106b, and the log thereof is described in the  
15 usage log data 308.

Then, the usage log data 308 is transmitted from the  
SAMs 305<sub>1</sub> to 305<sub>4</sub> to the EMD service center 302.

In the EMD service center 302, based on the usage  
log data 308, the charge content is determined  
20 (calculated) for each of the content providers 301a and  
301b and the service provider 310, and settlement claim  
data 152ca, 152cb, and 152s corresponding to them are  
produced based on the results thereof.

The EMD service center 302 transmits the settlement  
25 claim data 152ca, 152cb, and 152s via the payment gateway

90 to the settlement manager 91. By this, the money paid  
by the user of the user home network 303 to the  
settlement manager 91 is distributed to the owners of the  
content providers 301a and 301b and the service provider  
5 310.

As mentioned above, according to the EMD system  
300b, as the usage control policy data 106a and 106b of  
the content files CFa and CFb stored in the secure  
container 304, those produced by the content providers  
10 301a and 301b are used as they are, therefore, in the  
SAMs 305<sub>1</sub> to 305<sub>4</sub>, the rights for the content files CFa  
and CFb are reliably cleared based on the usage control  
policy data 106a and 106b according to the intention of  
the content providers 301a and 301b.

15 Note that, in the second modification shown in Fig.  
98, the case where two content providers were used was  
exemplified, but any number of the content providers may  
be used.

Further, there may be a plurality of both of the  
20 content providers and service providers.

#### Third modification of second embodiment

Figure 99 is a view of the configuration of the EMD  
system according to a third modification of the second  
embodiment.

25 In the second embodiment, the case where the EMD



service center 302 performed the settlement for the content provider 301 and the service provider 310 at the settlement manager 91 was exemplified, but in the present invention, for example, as shown in Fig. 99, it is also possible for the settlement claim data 152c for the content provider 301 and the settlement claim data 152s for the service provider 310 to be produced based on the usage log data 308 in the EMD service center 302 and for them to be transmitted to the content provider 301 and the service provider 310.

In this case, the content provider 301 performs settlement at a settlement manager 91a via a payment gateway 90a by using the settlement claim data 152c. Further, the service provider 310 performs settlement at a settlement manager 91b via a payment gateway 90b by using the settlement claim data 152s.

#### Fourth modification of second embodiment

Figure 100 is a view of the configuration of the EMD system according to a fourth modification of the second embodiment.

In the second embodiment, the case where the service provider 310 did not have a charging function as in for example the current Internet was exemplified, but where the service provider 310 has a charging function as in the current digital broadcast, in the CA module 311, a

usage log data 308s with respect to the service of the service provider 310 concerning the secure container 304 is produced and transmitted to the service provider 310.

Then, the service provider 310 performs charge  
5 processing based on the usage log data 308s to produce the settlement claim data 152s and performs settlement at the settlement manager 91b via the payment gateway 90b by using this.

On the other hand, the SAMs 305<sub>1</sub> to 305<sub>4</sub> produce  
10 usage log data 308c with respect to the rights clearing of the content provider 301 concerning the secure container 304 and transmit them to the EMD service center 302.

The EMD service center 302 produces the settlement  
15 claim data 152c based on the usage log data 308c and transmits this to the content provider 301.

The content provider 301 performs settlement at the settlement manager 91a via the payment gateway 90a by using the settlement claim data 152c.

20 Fifth modification of second embodiment

In the embodiment, as shown in Fig. 72, the case where the user preference filter data 903 was produced based on the usage log data 308 received from the SAM 305<sub>1</sub> etc. in the user preference filter generation unit  
25 901 of the EMD service center 302 was exemplified, but it

is also possible to produce for example the user preference filter data 903 in the user preference filter generation unit 901 based on the usage control status data 166 produced in the user monitor unit 186 of the SAM 305<sub>1</sub> shown in Fig. 78 and transmitted to the EMD service center 302 in real-time.

Sixth modification of second embodiment

The content provider 301, the service provider 310, and the SAMs 305<sub>1</sub> to 305<sub>4</sub> can register their secret key data  $K_{CP,S}$ ,  $K_{SP,S}$ , and  $K_{SAM1,S}$  to  $K_{SAM4,S}$  in the EMD service center 302 too other than their public key data  $K_{CP,P}$ ,  $K_{SP,P}$ , and  $K_{SAM1,P}$  to  $K_{SAM4,P}$ .

By doing this, it becomes possible for the EMD service center 302 to tap into desired communication among the communication between the content provider 301 and the service provider 310, the communication between the service provider 310 and the SAMs 305<sub>1</sub> to 305<sub>4</sub>, and the communication among the SAMs 305<sub>1</sub> to 305<sub>4</sub> in the user home network 303 by using the secret key data  $K_{CP,S}$ ,  $K_{SP,S}$ , and  $K_{SAM1,S}$  to  $K_{SAM4,S}$  in response to demands from the government or police organizations at the time of emergencies.

Further, for the SAMs 305<sub>1</sub> to 305<sub>4</sub>, it is also possible even if the secret key data  $K_{SAM1,S}$  to  $K_{SAM4,S}$  are produced by the EMD service center 302 at the time of

shipment, and they are stored in the SAMs 305<sub>1</sub> to 305<sub>4</sub> and, at the same time, held (registered) by the EMD service center 302.

Seventh modification of second embodiment

5        In the embodiment, the case where, when the content provider 301, service provider 310, and the SAMs 305<sub>1</sub> to 305<sub>4</sub> communicated with each other, the certificate data CER<sub>CP</sub>, CER<sub>SP</sub>, and CER<sub>SAM1</sub> to CER<sub>SAM4</sub> were acquired from the EMD service center 302 in advance and were transmitted to  
10      the destination of communication by the in-band method was exemplified, but in the present invention, various formats can be employed as the transmission format of the certificate data to the destination of communication.

For example, when the content provider 301, service  
15      provider 310, and the SAMs 305<sub>1</sub> to 305<sub>4</sub> communicate with each other, it is also possible if the certificate data CER<sub>CP</sub>, CER<sub>SP</sub>, and CER<sub>SAM1</sub> to CER<sub>SAM4</sub> are acquired from the EMD service center 302 in advance and are transmitted to the destination of communication by the in-band method  
20      preceding the related communication.

Further, it is also possible for the content provider 301, service provider 310, and the SAMs 305<sub>1</sub> to 305<sub>4</sub> to acquire the certificate data CER<sub>CP</sub>, CER<sub>SP</sub>, and CER<sub>SAM1</sub> to CER<sub>SAM4</sub> from the EMD service center 302 at the  
25      time of communication.

Figure 101 is a view for explaining the format of the route for acquiring (obtaining) the certificate data.

Note that, in Fig. 101, components given the same reference numerals as those of Fig. 59 are the same as the components having the same reference numerals explained above. Further, the user home network 303a is the same as the user home network 303 mentioned before. In a user home network 303b, SAMs 305<sub>11</sub> to 305<sub>14</sub> are connected via the IEEE1394 serial bus serving as the bus 191.

Where the content provider 301 acquires the certificate data  $CER_{sp}$  of the service provider 310, there are for example a case where the certificate data  $CER_{sp}$  is transmitted from the service provider 310 to the content provider 301 preceding the communication ((3) in Fig. 101) and a case where the content provider 301 orders the certificate data  $CER_{sp}$  from the EMD service center 302 ((1) in Fig. 101).

Also, where the service provider 310 acquires the certificate data  $CER_{cp}$  of the content provider 301, there are for example a case where the certificate data  $CER_{cp}$  is transmitted from the content provider 301 to the service provider 310 preceding the communication ((2) in Fig. 101) and a case where the service provider 310 orders the certificate data  $CER_{cp}$  from the EMD service

center 302 ((4) in Fig. 101).

Also, where the service provider 310 acquires the certificate data  $CER_{SAM1}$  to  $CER_{SAM4}$  of the SAMs  $305_1$  to  $305_4$ , there are for example a case where the certificate data  $CER_{SAM1}$  to  $CER_{SAM4}$  are transmitted from the SAMs  $305_1$  to  $305_4$  to the service provider 310 preceding the communication ((6) in Fig. 101) and a case where the service provider 310 orders the certificate data  $CER_{SAM1}$  to  $CER_{SAM4}$  from the EMD service center 302 ((4) in Fig. 101).

Also, where the SAMs  $305_1$  to  $305_4$  acquire the certificate data  $CER_{SP}$  of the service provider 310, there are for example a case where the certificate data  $CER_{SP}$  is transmitted from the service provider 310 to the SAMs  $305_1$  to  $305_4$  preceding the communication ((5) in Fig. 101) and a case where the SAMs  $305_1$  to  $305_4$  order the certificate data  $CER_{SP}$  from the EMD service center 302 ((7) in Fig. 101, etc.).

Also, where the SAM  $305_1$  acquires the certificate data  $CER_{SAM2}$  of the SAM  $305_2$ , there are for example a case where the certificate data  $CER_{SAM2}$  is transmitted from the SAM  $305_2$  to the SAM  $305_1$  preceding the communication ((8) in Fig. 101) and a case where the SAM  $305_1$  orders the certificate data  $CER_{SAM2}$  from the EMD service center 302 ((7) in Fig. 101, etc.).

Also, where the SAM  $305_2$  acquires the certificate

data  $CER_{SAM1}$  of the SAM 305<sub>1</sub>, there are for example a case where the certificate data  $CER_{SAM1}$  is transmitted from the SAM 305<sub>1</sub> to the SAM 305<sub>2</sub> preceding the communication ((9) in Fig. 101), a case where the SAM 305<sub>2</sub> orders the

5 certificate data  $CER_{SAM1}$  from the EMD service center 302 by itself, and a case where the SAM 305<sub>2</sub> orders the certificate data  $CER_{SAM1}$  via the network apparatus with the SAM 305<sub>1</sub> mounted thereon ((7) and (8) in Fig. 101).

Also, where the SAM 305<sub>4</sub> acquires certificate data

10  $CER_{SAM13}$  of the SAM 305<sub>13</sub>, there are for example a case where the certificate data  $CER_{SAM13}$  is transmitted from the SAM 305<sub>13</sub> to the SAM 305<sub>4</sub> preceding the communication ((12) in Fig. 101), a case where the SAM 305<sub>4</sub> orders the certificate data  $CER_{SAM13}$  from the EMD service center 302

15 by itself ((10) in Fig. 101), and a case where the SAM 305<sub>4</sub> orders the certificate data  $CER_{SAM13}$  via the network apparatus in the user home network 303b.

Also, where the SAM 305<sub>13</sub> acquires the certificate data  $CER_{SAM4}$  of the SAM 305<sub>4</sub>, there are for example a case

20 where the certificate data  $CER_{SAM4}$  is transmitted from the SAM 305<sub>4</sub> to the SAM 305<sub>13</sub> preceding the communication ((11) in Fig. 101), a case where the SAM 305<sub>13</sub> orders the certificate data  $CER_{SAM4}$  from the EMD service center 302 by itself ((13) in Fig. 101), and a case where the SAM

25 305<sub>13</sub> orders the certificate data  $CER_{SAM4}$  via the network

apparatus in the user home network 303b.

Handling of certificate revocation list (data) in  
second embodiment

In the second embodiment, in order to prevent the  
5 content provider 301, service provider 310, and the SAMs  
305<sub>1</sub> to 305<sub>4</sub> used for illegitimate action etc. from  
communicating with the other apparatuses in the EMD  
service center 302, a certificate revocation list for  
invalidating the certificate data of the apparatus used  
10 for the related illegitimate action is produced. Then,  
the related certificate revocation list CRL is  
transmitted to the content provider 301, service provider  
310, and the SAMs 305<sub>1</sub> to 305<sub>4</sub>.

Note that, it is also possible if the certificate  
15 revocation list CRL is produced in for example the  
content provider 301, service provider 310, and the SAMs  
305<sub>1</sub> to 305<sub>4</sub> other than the EMD service center 302.

First, an explanation will be made of the case where  
the EMD service center 302 invalidates the certificate  
20 data CER<sub>CP</sub> of the content provider 301.

As shown in Fig. 102, the EMD service center 302  
transmits a certificate revocation list CRL<sub>1</sub> indicating  
the invalidation of the certificate data CER<sub>CP</sub> to the  
service provider 310 ((1) in Fig. 102). When verifying  
25 the signature data input from the content provider 301,



the service provider 310 decides the validity of the certificate data  $CER_{CP}$  by referring to the certificate revocation list  $CRL_1$ , performs signature verification using the public key data  $K_{CP,P}$  where it decides that it is valid, while invalidates the data from the content provider 301 without the related signature verification where it decides that it is invalid. Note that, it is also possible not to invalidate the data, but reject the communication.

Also, the EMD service center 302 transmits the certificate revocation list  $CRL_1$  to for example the SAM 305<sub>1</sub> in the user home network 303 by utilizing circulation resources of the service provider 310 by either the broadcast type or on-demand type ((1) and (2) in Fig. 102). When verifying the signature data of the content provider 301 stored in the secure container input from the service provider 310, the SAM 305<sub>1</sub> decides the validity of the certificate data  $CER_{CP}$  by referring to the certificate revocation list  $CRL_1$ , performs signature verification using the public key data  $K_{CP,P}$  where it decides it as valid, while invalidates the related secure container without the related signature verification where it decides it as invalid.

Note that, it is also possible for the EMD service center 302 to directly transmit the certificate

revocation list  $CRL_1$  to the SAM 305<sub>1</sub> via the network apparatus in the user home network 303 ((3) in Fig. 102).

Next, an explanation will be made of the case where the EMD service center 302 invalidates the certificate data  $CER_{sp}$  of the service provider 310.

As shown in Fig. 103, the EMD service center 302 transmits a certificate revocation list  $CRL_2$  indicating the invalidation of the certificate data  $CER_{sp}$  to the content provider 301 ((1) in Fig. 103). When verifying the signature data input from the service provider 310, the content provider 301 decides the validity of the certificate data  $CER_{sp}$  by referring to the certificate revocation list  $CRL_2$ , performs signature verification using the public key data  $K_{sp,p}$  where it decides it as valid, while invalidates the data from the service provider 310 without the related signature verification where it decides it as invalid.

Also, the EMD service center 302 transmits the certificate revocation list  $CRL_2$  to for example the SAM 305<sub>1</sub> in the user home network 303 by utilizing the circulation resources of the service provider 310 by either the broadcast type or on-demand type ((2) in Fig. 103). When verifying the signature data of the content provider 301 stored in the secure container input from the service provider 310, the SAM 305<sub>1</sub> decides the

validity of the certificate data  $CER_{SP}$  by referring to the certificate revocation list  $CRL_2$ , performs signature verification using the public key data  $K_{SP,P}$  where it decides it as valid, and while invalidates the related  
5 secure container without the related signature verification where it decides it as invalid.

In this case, in the service provider 310, the module for transmitting and receiving the certificate revocation list  $CRL_2$  must have tamper resistance.  
10 Further, in the service provider 310, the certificate revocation list  $CRL_2$  must be stored in a region where tampering by an interested party of the service provider 310 is difficult.

Note that, it is also possible for the EMD service  
15 center 302 to directly transmit the certificate revocation list  $CRL_2$  to the SAM 305<sub>1</sub> via the network apparatus in the user home network 303 ((3) in Fig. 103).

Next, an explanation will be made of a case where the EMD service center 302 invalidates for example the  
20 certificate data  $CER_{SAM2}$  of the SAM 305<sub>2</sub>.

As shown in Fig. 104, the EMD service center 302 transmits a certificate revocation list  $CRL_3$  indicating the invalidation of the certificate data  $CER_{SAM2}$  to the content provider 301 ((1) in Fig. 104). The content  
25 provider 301 transmits the certificate revocation list

CRL<sub>3</sub> to the service provider 310. The service provider 310 transmits the certificate revocation list CRL<sub>3</sub> to for example the SAM 305<sub>1</sub> in the user home network 303 by utilizing its own circulation resources by either the  
5 broadcast type or on-demand type ((1) in Fig. 104). When verifying the signature data of the SAM 305<sub>2</sub> added to the data input from the SAM 305<sub>2</sub>, the SAM 305<sub>1</sub> decides the validity of the certificate data CER<sub>SAM2</sub> by referring to the certificate revocation list CRL<sub>3</sub>, performs signature  
10 verification using the public key data K<sub>SAM2,P</sub> where it decides it as valid, while invalidates the related data without the related signature verification where it decides it as invalid.

In this case, in the service provider 310, the  
15 module for transmitting and receiving the certificate revocation list CRL<sub>3</sub> must have tamper resistance. Further, in the service provider 310, the certificate revocation list CRL<sub>3</sub> must be stored in a region where tampering by an interested party of the service provider  
20 310 is difficult.

It is also possible for the EMD service center 302 to transmit the certificate revocation list CRL<sub>3</sub> to the SAM 305<sub>1</sub> via the service provider 310 ((1) and (2) in Fig. 104).

25 Further, it is also possible for the EMD service

center 302 to directly transmit the certificate  
revocation list  $CRL_3$  to the SAM 305<sub>1</sub> via the network  
apparatus in the user home network 303 ((3) in Fig. 104).

Also, the EMD service center 302 produces and stores  
5 the certificate revocation list  $CRL_3$  indicating the  
invalidation of for example the certificate data  $CER_{SAM2}$   
of the SAM 305<sub>2</sub>.

Also, the user home network 303 produces a SAM  
registration list SRL of the SAMs connected to the bus  
10 191 and transmits this to the EMD service center 302 ((1)  
in Fig. 105).

The EMD service center 302 specifies the SAMs (for  
example SAM 305<sub>2</sub>) for which invalidation is instructed by  
the certificate revocation list  $CRL_3$  among the SAMs 305<sub>1</sub>  
15 to 305<sub>4</sub> indicated in the SAM registration list, sets  
revocation flags corresponding to the related SAMs in the  
SAM registration list SRL so as to indicate the  
invalidity, and produces a new SAM registration list SRL.

Next, the EMD service center 302 transmits the  
20 related produced SAM registration list SRL to the SAM  
305<sub>1</sub> ((1) in Fig. 105).

The SAM 305<sub>1</sub> determines the existence of the  
verification of the signature data and whether or not  
communication is permitted by referring to the revocation  
25 flags of the SAM registration list SRL when communicating

with another SAM.

Also, the EMD service center 302 produces the certificate revocation list  $CRL_3$  and transmits this to the content provider 301 ((2) in Fig. 105).

5       The content provider 301 transmits the certificate revocation list  $CRL_3$  to the service provider 310 ((2) in Fig. 105).

Next, the service provider 310 transmits the certificate revocation list  $CRL_3$  to the SAM 305<sub>1</sub> by  
10 either the broadcast type or on-demand type by utilizing its own circulation resources ((2) in Fig. 105).

The SAM 305<sub>1</sub> specifies the SAMs (for example SAM 305<sub>2</sub>) for which invalidation is instructed by the certificate revocation list  $CRL_3$  among the SAMs 305<sub>1</sub> to  
15 305<sub>4</sub> indicated in the SAM registration list produced by itself and sets revocation flags corresponding to the related SAMs in the SAM registration list SRL so as to indicate the invalidity.

From then on, the SAM 305<sub>1</sub> determines the existence  
20 of verification of the signature data and whether or not communication is permitted by referring to the revocation flag of the related SAM registration list SRL when communicating with another SAM.

Also, the EMD service center 302 produces the  
25 certificate revocation list  $CRL_3$  and transmits this to

the service provider 310 ((3) in Fig. 105).

Next, the service provider 310 transmits the  
certificate revocation list CRL<sub>3</sub> to the SAM 305<sub>1</sub> by  
either the broadcast type or on-demand type by utilizing  
5 its own circulation resources ((3) in Fig. 105).

The SAM 305<sub>1</sub> specifies the SAMs (for example SAM  
305<sub>2</sub>) for which invalidation is instructed by the  
certificate revocation list CRL<sub>3</sub> among the SAMs 305<sub>1</sub> to  
305<sub>4</sub> indicated in the SAM registration list produced by  
10 itself and sets revocation flags corresponding to the  
related SAMs in the SAM registration list SRL so as to  
indicate the invalidity.

From then on, the SAM 305<sub>1</sub> determines the existence  
of verification of the signature data and whether or not  
15 communication is permitted by referring to the revocation  
flag of the related SAM registration list SRL when  
communicating with another SAM.

#### Role etc. of EMD service center 302

Figure 106 is a view of the configuration of the EMD  
20 system where the functions of the EMD service center  
(clearinghouse) 302 shown in Fig. 59 are divided between  
a right management use clearinghouse 950 and an  
electronic settlement use clearinghouse 951.

In the related EMD system, in the electronic  
25 settlement use clearinghouse 951, settlement processing

(profit distribution processing) is carried out based on the usage log data 308 from the SAM of the user home networks 303a and 303b, settlement claim data of the content provider 301 and the service provider 310 are  
5 produced, and settlement is carried out at the settlement manager 91 via the payment gateway 90.

Also, the right management use clearinghouse 950 produces the settlement reports of the content provider 301 and the service provider 310 in accordance with the  
10 settlement notification from the electronic settlement use clearinghouse 951 and transmits them to the content provider 301 and the service provider 310.

Also, it performs the registration (authentication) etc. of the usage control policy data 106 and the content  
15 key data Kc of the content provider 301.

Note that, as shown in Fig. 107, when the right management use clearinghouse 950 and the electronic settlement use clearinghouse 951 are accommodated in a single apparatus, the EMD service center 302 shown in  
20 Fig. 59 is formed.

Also, in the present invention, for example, it is also possible to provide the function of a right management use clearinghouse 960 in the EMD service center 302, perform the registration etc. of the usage  
25 control policy data 106 in the right management use



clearinghouse 960 and, at the same time, produce the settlement claim data of the service provider 310 based on the usage log data 308 from the SAMs and transmit this to the service provider 310 as shown in Fig. 108. In this case, the service provider 310 utilizes its own charge system as an electronic settlement use clearinghouse 961 and performs settlement based on the settlement claim data from the right management use clearinghouse 960.

Also, in the present invention, for example, it is also possible to provide the function of a right management use clearinghouse 970 in the EMD service center 302, perform the registration etc. of the usage control policy data 106 in the right management use clearinghouse 970 and, at the same time, produce the settlement claim data of the content provider 301 based on the usage log data 308 from the SAMs and transmit this to the content provider 301 as shown in Fig. 109. In this case, the content provider 301 utilizes its own charge system as an electronic settlement use clearinghouse 971 and performs settlement based on the settlement claim data from the right management use clearinghouse 970.

Also, in the present invention, for example, it is also possible to provide the function of the right management use clearinghouse 970 and the electronic settlement use clearinghouse 971 mentioned above in the

content provider 301 as shown in Fig. 110.

In this case, the content provider 301 utilizes its own charge system as the electronic settlement use clearinghouse 961 and performs settlement by itself at the settlement manager 91 based on the settlement claim data produced in the right management use clearinghouse 970.

Eighth modification of the second embodiment

In the second embodiment, the case where the secure container 104 of the format shown in Fig. 5 was provided from the content provider 301 to the service provider 310, and the secure container 304 of the format shown in Fig. 65 was distributed from the service provider 310 to the user home network 303 in the EMD system 300 shown in Fig. 59 was exemplified.

Namely, in the second embodiment, the case where a single content file CF and a single key file KF corresponding to the related content file CF were stored in the secure container 104 and the secure container 304 as shown in Fig. 5 and Fig. 65 was exemplified.

In the present invention, it is also possible to store a plurality of content files CF and a plurality of key files KF corresponding to the related plurality of content files CF in the secure container 104 and the secure container 304.

Figure 111 is a view for explaining the format of the secure container 104a provided from the content provider 301 to the service provider 310 shown in Fig. 59 in the present modification.

5       As shown in Fig. 111, in the secure container 104a, content files  $CF_1$ ,  $CF_2$ , and  $CF_3$ , key files  $KF_1$ ,  $KF_2$ , and  $KF_3$ , certificate data  $CER_{CP}$ , and signature data  $SIG_{200,CP}$ ,  $SIG_{201,CP}$ ,  $SIG_{202,CP}$ ,  $SIG_{203,CP}$ ,  $SIG_{204,CP}$ ,  $SIG_{205,CP}$ , and  $SIG_{1,ESC}$  are stored.

10       Here, the signature data  $SIG_{200,CP}$ ,  $SIG_{201,CP}$ ,  $SIG_{202,CP}$ ,  $SIG_{203,CP}$ ,  $SIG_{204,CP}$ , and  $SIG_{205,CP}$  are produced in the content provider 301 by taking the hash values of the content files  $CF_1$ ,  $CF_2$ , and  $CF_3$  and the key files  $KF_1$ ,  $KF_2$ , and  $KF_3$ , and using the secret key data  $K_{CP,S}$  of the content  
15       provider 301.

In the content file  $CF_1$ , a header, meta data  $Meta_1$ , content data  $C_1$ , an A/V expansion use software  $Soft_1$ , and a watermark module  $WM_1$  are stored.

Here, the content data  $C_1$  and the A/V expansion use  
20       software  $Soft_1$  have been encrypted by using the content key data  $Kc_1$ , and the meta data  $Meta_1$  and the watermark module  $WM_1$  have been encrypted by using the content key data  $Kc_1$  according to need.

Also, the content data  $C_1$  has been compressed by for  
25       example the ATRAC3 method. The A/V expansion use software

Soft<sub>1</sub> is the software for the expansion of the ATRAC3 method.

Also, in the header of the content file CF<sub>1</sub>, for example, as shown in Fig. 112, directory structure data  
5 DSD<sub>1</sub> indicating the linkage to the key file KF<sub>1</sub> and the content file CF<sub>2</sub> is contained.

In the content file CF<sub>2</sub>, the header, meta data Meta<sub>2</sub>, content data C<sub>2</sub>, an A/V expansion use software Soft<sub>2</sub>, and a watermark module WM<sub>2</sub> are stored.

10 Here, the content data C<sub>2</sub> and the A/V expansion use software Soft<sub>2</sub> have been encrypted by using the content key data Kc<sub>2</sub>, and the meta data Meta<sub>2</sub> and the watermark module WM<sub>2</sub> have been encrypted by using the content key data Kc<sub>2</sub> according to need.

15 Also, the content data C<sub>2</sub> has been compressed by for example the MPEG2 method. The A/V expansion use software Soft<sub>2</sub> is the software for the expansion of the MPEG2 method.

Also, in the header of the content file CF<sub>2</sub>, for  
20 example, as shown in Fig. 112, directory structure data DSD<sub>2</sub> indicating the linkage to the key file KF<sub>2</sub> and the content file CF<sub>3</sub> is contained.

In the content file CF<sub>3</sub>, the header, meta data Meta<sub>3</sub>, content data C<sub>3</sub>, an A/V expansion use software  
25 Soft<sub>3</sub>, and a watermark module WM<sub>3</sub> are stored.

Here, the content data  $C_3$  and the A/V expansion use software  $Soft_3$  have been encrypted by using the content key data  $Kc_3$ , and the meta data  $Meta_3$  and the watermark module  $WM_3$  have been encrypted by using the content key data  $Kc_3$  according to need.

Also, the content data  $C_3$  has been compressed by for example the JPEG method. The A/V expansion use software  $Soft_3$  is the software for the expansion of the JPE G method.

Also, in the header of the content file  $CF_2$ , for example, as shown in Fig. 112, directory structure data  $DSD_3$  indicating the linkage to the key file  $KF_3$  is contained.

In the key file  $KF_1$ , the header, content key data  $Kc_1$  encrypted by using the distribution use key data  $KD_1$  to  $KD_3$ , usage control policy data  $106_1$ , the SAM program download container  $SDC_1$ , and signature data  $SIG_{220,ESC}$  are stored.

In the key file  $KF_2$ , the header, content key data  $Kc_2$  encrypted by using the distribution use key data  $KD_1$  to  $KD_3$ , usage control policy data  $106_2$ , the SAM program download container  $SDC_2$ , and signature data  $SIG_{221,ESC}$  are stored.

In the key file  $KF_3$ , the header, content key data  $Kc_3$  encrypted by using the distribution use key data  $KD_1$

to  $KD_3$ , usage control policy data  $106_3$ , the SAM program download container  $SDC_3$ , and signature data  $SIG_{222,ESC}$  are stored.

When receiving the secure container 104a shown in Fig. 112, the service provider 310 confirms the legitimacy of the signature data  $SIG_{200,CP}$ ,  $SIG_{201,CP}$ ,  $SIG_{202,CP}$ ,  $SIG_{203,CP}$ ,  $SIG_{204,CP}$ , and  $SIG_{205,CP}$ , that is, the legitimacy of the producers and transmitters of the content files  $CF_1$ ,  $CF_2$ , and  $CF_3$ , and the legitimacy of the transmitters of the key files  $KF_1$ ,  $KF_2$ , and  $KF_3$  by using the public key data  $K_{CP,P}$  stored in the certificate data  $CER_{CP}$  after confirming the legitimacy of the related certificate data  $CER_{CP}$  by using the public key data  $K_{ESC,P}$  of the EMD service center 302.

Also, the content provider 301 confirms the legitimacy of the signature data  $SIG_{220,ESC}$ ,  $SIG_{221,ESC}$ , and  $SIG_{222,ESC}$  and the legitimacy of the producers of the key files  $KF_1$ ,  $KF_2$ , and  $KF_3$  by using the public key data  $K_{ESC,P}$ .

Then, the service provider 310 produces price tag data  $312_1$ ,  $312_2$ , and  $312_3$  indicating the sales prices of the content files  $CF_1$ ,  $CF_2$ , and  $CF_3$ .

Also, the service provider 310 produces the signature data  $SIG_{220,SP}$ ,  $SIG_{221,SP}$ , and  $SIG_{222,SP}$  of the price tag data  $312_1$ ,  $312_2$ , and  $312_3$  by using the secret key data  $K_{SP,S}$ .

Also, the service provider 310 produces the signature data  $SIG_{210,SP}$ ,  $SIG_{211,SP}$ ,  $SIG_{212,SP}$ ,  $SIG_{213,SP}$ ,  $SIG_{214,SP}$ , and  $SIG_{215,SP}$  of the content files  $CF_1$ ,  $CF_2$ , and  $CF_3$  and  $KF_1$ ,  $KF_2$ , and  $KF_3$  by using the secret key data  $K_{SP,S}$ .

5       Next, the service provider 310 produces the secure container 304a shown in Fig. 114.

The service provider 310 distributes the secure container 304a shown in Fig. 114 to the user home network 303.

10       In the user home network 303, in the SAMs 305<sub>1</sub> to 305<sub>4</sub>, after confirming the legitimacy of all signature data stored in the secure container 304a, the rights for the content data  $C_1$ ,  $C_2$  and  $C_3$  are cleared in accordance with the link state shown in the directory structure data  
15   DSD<sub>1</sub> to DSD<sub>3</sub> based on the key files  $KF_1$ ,  $KF_2$ , and  $KF_3$ .

Also, in the eighth modification mentioned above, in the secure container 304, the case where the plurality of content files  $CF_{101}$ ,  $CF_{102}$ , and  $CF_{103}$  provided from the single service provider 310 were stored in the single  
20   secure container 304a and distributed to the user home network 303 was exemplified. but as shown in Fig. 98, it is also possible to store a plurality of content files  $CF$  provided from a plurality of content providers 301a and 301b in a single secure container and distribute the same  
25   to the user home network 303.

Also, in the secure containers 104 and 304, for example, as shown in Fig. 113, it is also possible if a content file CF<sub>1</sub> storing music (voice) data compressed by the ATRAC3, a content file CF<sub>2</sub> storing video clip data compressed by the MPEG2, a content file CF<sub>3</sub> storing the jacket (still image) data compressed by the JPEG, a content file CF<sub>4</sub> storing the lyrics data in a text format, and a content file CF<sub>5</sub> storing the liner note data in a text format and key files KF<sub>1</sub>, KF<sub>2</sub>, KF<sub>3</sub>, KF<sub>4</sub> and KF<sub>5</sub> corresponding to them are stored.

Also in this case, similarly, by the directory structure data of the content files CF<sub>1</sub> to CF<sub>5</sub>, the linkage among the content files CF<sub>1</sub> to CF<sub>5</sub> and the linkage between the content files CF<sub>1</sub> to CF<sub>5</sub> and the key files KF<sub>1</sub> to KF<sub>5</sub> are established.

Note that, the concept of the data format in the case where a plurality of content data are stored in the secure container in the present embodiment (case of composite type) is shown in for example Fig. 115 or Fig. 116.

Note that, the format shown in Fig. 111 can be similarly applied to also the case where the secure container 104 is transmitted from the content provider 101 to the user home network 103 shown in Fig. 1.

Ninth modification of second embodiment



In the above embodiment, the case where the content files CF and the key files KF were stored in the secure containers 104 and 304 with the directory structures and transmitted from the content provider 301 to the service provider 310 and from the service provider 310 to the SAMs 305<sub>1</sub> to 305<sub>4</sub>, was exemplified, but it is also possible to separately transmit the content files CF and key files KF from the content provider 301 to the service provider 310 and from the service provider 310 to the SAMs 305<sub>1</sub> to 305<sub>4</sub>.

This includes for example the following first technique and second technique.

In the first technique, as shown in Fig. 117, the content files CF and the key files KF are separately transmitted from the content provider 301 to the service provider 310 and from the service provider 310 to the SAMs 305<sub>1</sub> to 305<sub>4</sub>.

Also, in the second technique, as shown in Fig. 118, the content files CF are transmitted from the content provider 301 to the service provider 310 and from the service provider 310 to the SAMs 305<sub>1</sub> to 305<sub>4</sub>, and the key files KF are transmitted from the EMD service center 302 to the SAMs 305<sub>1</sub> to 305<sub>4</sub>. The related key files KF are transmitted from the EMD service center 302 to the SAMs 305<sub>1</sub> to 305<sub>4</sub>, when for example the users of the SAMs

305<sub>1</sub> to 305<sub>4</sub> are going to determine the purchase form of the content data C.

Where the first technique and the second technique are employed, for example, a link is established between related content files CF and between the content files CF and the key files KF corresponding to them by using the hyper link data HL stored in the headers of at least one of the content files CF and the key files KF. In the SAMs 105<sub>1</sub> to 105<sub>4</sub>, the rights are cleared and the content data C is used based on the related link.

Also, in the above second embodiment, the case where the content data C and the key data such as the content key data Kc and the usage control policy data 106 were transmitted from the content provider 301 to the service provider 310 and from the service provider 310 to the SAMs 305<sub>1</sub> to 305<sub>4</sub> in the file format was exemplified, but it is not always necessary to comprise them in the file format so far as the link among them can be established.

For example, as shown in Fig. 119, it is also possible to separately transmit the content data C, meta data Meta, A/V expansion use software Soft, watermark module WM, key file KF, price tag data 312, and the certificate data CER<sub>CP</sub> and CER<sub>SP</sub> from the content provider 301 and the EMD service center 302 to the SAMs 305<sub>1</sub> to 305<sub>4</sub>.

In this case, as shown in Fig. 119, the content data C, meta data Meta, A/V expansion use software Soft, watermark module WM, key file KF, price tag data 312, and certificate data  $CER_{CP}$  and  $CER_{SP}$  are linked by the hyper  
5 link data HL.

Here, the hyper link data HL is encrypted by for example the distribution use key data  $KD_1$  to  $KD_6$  and transmitted.

Note that, in the present modification, as the  
10 formats of the content files CF and the key files KF, for example those shown in Figs. 5A and 5B are employed. Also, in this case, preferably the signature data  $SIG_{6,CP}$  and  $SIG_{7,CP}$  of them are transmitted together with the content files CF and the key files KF.

15 10th modification of second embodiment

In the above embodiment, the case where the content files CF and the key files KF were separately provided in the secure container 104 was exemplified, but for  
example, as shown in Fig. 120, it is also possible to  
20 store the key files KF in the content files CF in the secure containers 104 and 304.

In this case, with respect to the content files CF storing the key files KF, the signature data by the secret key data  $K_{CP,S}$  of the content provider 301 and the  
25 signature by the secret key data  $K_{SP,S}$  of the service

provider 310 are attached.

11th modification of second embodiment

In the above embodiment, the case where the content data C was stored in the content files CF, the content key data Kc and the usage control policy data 106 were stored in the key files KF, and they were transmitted from the content provider 301 to the service provider 310 and from the service provider 310 to the SAM 305<sub>1</sub> etc. was exemplified, but it is also possible to transmit at least one among the content data C, content key data Kc, and usage control policy data 106 from the content provider 301 to the service provider 310 and from the service provider 310 to the SAMs 305<sub>1</sub> etc. in a format not depending upon the communication protocol without employing the file format.

For example, as shown in Fig. 121, in the content provider 301, the secure container 104s storing the content data C encrypted by the content key data Kc and the key file KF containing the encrypted content key data Kc and the encrypted usage control policy data 106 etc. is produced, and the secure container 104s is transmitted to the service provider 310 in a format not depending upon the communication protocol. Then, in the service provider 310, it is also possible if the price tag data 312 is added to the content data C and the key file KF

stored in the secure container 104s to produce the secure container 304s, and the secure container 304s is transmitted to the SAM 305<sub>1</sub> etc. in a format not depending upon the communication protocol.

5       Also, as shown in Fig. 122, the content data C encrypted by the content key data Kc and the key file KF containing the encrypted content key data Kc and the encrypted usage control policy data 106 etc. are separately transmitted from the content provider 301 to  
10   the service provider 310 in a format not depending upon the communication protocol. Then, from the service provider 310 to the SAM 305<sub>1</sub> etc., the content data C, key file KF, and the price tag data 312 are separately transmitted in a format not depending upon the  
15   communication protocol. Namely, the content data C is not comprised in the file format and is transmitted by the identical route to that for the key file KF.

      Also, as shown in Fig. 123, the content data C encrypted by the content key data Kc is transmitted from  
20   the content provider 301 to the service provider 310 in a format not depending upon the communication protocol, while the content data C and the price tag data 312 are transmitted from the service provider 310 to the SAM  
305<sub>1</sub> etc. in a format not depending upon the  
25   communication protocol. Also, it is also possible if the

key file KF containing the encrypted content key data Kc and the encrypted usage control policy data 106 etc. is transmitted from the EMD service center 302 to the SAM 305<sub>1</sub> etc. Namely, the content data C is not comprised in  
5 the file format and is transmitted by a different route from that for the key file KF.

Also, as shown in Fig. 124, the content data C encrypted by the content key data Kc, the content key data Kc, and the usage control policy data 106 are  
10 transmitted from the content provider 301 to the service provider 310 in a format not depending upon the communication protocol. Also, the content data C, content key data Kc, usage control policy data 106, and the price tag data 312 are transmitted from the service provider  
15 310 to the SAM 305<sub>1</sub> etc. Namely, the content data C, content key data Kc, usage control policy data 106, and the price tag data 312 are transmitted not in the file format and by the same route.

Also, as shown in Fig. 125, the content data C encrypted by the content key data Kc is transmitted from  
20 the content provider 301 to the service provider 310 in a format not depending upon the communication protocol. Then, the content data C and the price tag data 312 are transmitted from the service provider 310 to the SAM 305<sub>1</sub>  
25 etc. in a format not depending upon the communication

protocol. Also, the content key data Kc and the usage  
control policy data 106 are transmitted from the EMD  
service center 302 to the SAM 305<sub>1</sub> etc. Namely, the  
content data C, content key data Kc, and the usage  
5 control policy data 106 are transmitted not in the file  
format and by different routes.

12th modification of second embodiment

In the EMD system 300 shown in Fig. 59 mentioned  
above, for example, as shown in Fig. 126, the user home  
10 network 303 can distribute a secure container 304A in  
accordance with the secure container 304 received from  
the service provider 310 to the user home network 303a in  
response to a request S303a from a SAM of the user home  
network 303a too.

15 In this case, it can be considered that the SAM of  
the user home network 303 functions in the same way as  
the service provider 310 explained in the second  
embodiment.

In this case, the SAM of the user home network 303a  
20 can uniquely newly set the price tag data 312.

Then, the purchase form of the content data C is  
determined in the SAM of the user home network 303a, and  
the usage log data 304a etc. in accordance with that are  
transmitted from the SAM of the user home network 303a to  
25 the EMD service center 302.

In the EMD service center 302, based on the usage log data 304a, the settlement processing for distributing the money paid by the user of the user home network 303a to the user of the content provider 301, service provider 310, and user home network 303 is carried out.

Note that, the file inclusion size relationships of the secure containers in the present embodiment can be expressed as shown in Fig. 127.

#### Third embodiment

Figure 128 is a view for explaining the EMD system of a third embodiment of the present invention, while Fig. 129 is a functional block diagram of the EMD service center shown in Fig. 128.

In Fig. 129, components given the same reference numerals as those used in the above first embodiment and second embodiment are the same as the components having the same reference numerals explained in these embodiments.

In the EMD system of the present embodiment, the content provider 301 sends the master source (content data) S111 etc. to the EMD service center 302, and for example the content file CF shown in Fig. 5A is produced in the EMD service center 302.

Also, the content provider 301 sends the content ID, content key data Kc, and the electronic watermark



management information (contents of the electronic watermark information buried in the content data) of the content data S111, the identifier CP\_ID of the content provider 301, the identifier SP\_ID of the service provider 310, and the suggested retailer's price SRP of the content data to the EMD service center 302, and the key file KF shown in Fig. 5B is produced in the EMD service center 302.

Also, the EMD service center 302 stores the produced content file CF in the CF database 802a, attaches global unique content IDs to the individual content files CF, and centrally manages them. Also, the EMD service center 302 stores the key file KF in the KF database 153a and centrally manages also this by using the content ID.

An explanation will be made of the processing in the EMD service center 302 by referring to Fig. 129.

The EMD service center 302 stores the master source S111 received from the content provider 301 in the content master source database 801.

Next, in the electronic watermark information addition unit 112, the electronic watermark information indicated by the electronic watermark management information received from the content provider 301 is buried in the master source S111 read out from the content master source database 810 to produce the content

data S112.

Next, in the compression unit 113, the content data S112 is compressed to produce the content data S113.

The content data S112 is expanded at the expansion  
5 unit 116 and then checked audially in the audial check  
unit 123. If necessary, the electronic watermark  
information is buried again by the electronic watermark  
information addition unit 112.

Next, in the encryption unit 114, the content data  
10 S113 is encrypted by using the content key data Kc to  
produce the content data S114.

Next, in the CF preparation unit 802, the content  
file CF shown in Fig. 5A storing the content data S114  
etc. is produced, and the content file CF is stored in a  
15 CF database 802a.

Also, in the EMD service center 302, in the KF  
preparation unit 153, the key file KF shown in Fig. 5B is  
produced, and the key file KF is stored in a KF database  
153a.

20 Next, in the secure container preparation unit 804,  
a secure container 806 storing the content file CF read  
out from the CF database 802a and the key file KF read  
out from the KF database 153a is produced, and the secure  
container 806 is stored in the secure container database  
25 805.

Thereafter, the secure container database 805 is accessed by the service provider 310, and the secure container 806 is supplied to the service provider 310.

Next, the service provider 310 produces a secure  
5 container 807 storing the content file CF and key file KF stored in the secure container 806 and the price tag data 312 indicating the sales price of the content data.

Then, the service provider 310 distributes the secure container 807 to the user home network 303 by  
10 using the predetermined communication protocol and in a format not depending upon the related communication protocol or by storing the same in a storage medium.

In the user home network 303, in the case of on-line, the secure container 807 is provided to the SAM  
15 305<sub>1</sub> etc. via the CA module 311, in the SAM 305<sub>1</sub> etc., the content key data Kc, usage control policy data 106, etc. stored in the key file KF are decrypted by using the distribution use key data KD<sub>1</sub> to KD<sub>3</sub> or the like, and the handling such as the purchase form of the content data  
20 stored in the content file CF is determined based on the decrypted usage control policy data 106.

Also, in the SAM 305<sub>1</sub> etc., the usage log data 308 indicating the purchase log etc. of the content data is produced, and the usage log data 308 is transmitted to  
25 the EMD service center 302.

Also, where the secure container 807 is distributed from the SAM 305<sub>2</sub> of the user home network 303 to the SAM 305<sub>12</sub> of the user home network 303a, processing similar to that in the SAM 305<sub>2</sub> is carried out in the SAM 305<sub>12</sub>,  
5 and the usage log data 308 is transmitted from the SAM 305<sub>12</sub> to the EMD service center 302.

Note that, the processings with respect to the secure container 807 in the user home networks 303 and 303a are the same as the processings in the user home  
10 networks 103 and 303 in the first embodiment and second embodiment mentioned above.

Also, in the example shown in Fig. 128, the case where the secure container storing the content file CF and the key file KF was transmitted from the EMD service  
15 center 302 to the service provider 310 and from the service provider 310 to the user home network 303 (the case of in-band) was exemplified, but it is also possible to separately transmit the content file CF and the key file KF by the same route (the case of out-of-band).

Also, as shown in Fig. 130, it is also possible if  
20 the content file CF produced in the EMD service center 302 is supplied to the service provider 310, the service provider 310 supplies the content file CF to the user home network 303 and, at the same time, the key file KF  
25 produced in the EMD service center 302 is supplied from

the EMD service center 302 to the SAM 305<sub>2</sub> and SAM 305<sub>12</sub> of the user home networks 303 and 303a.

Fourth embodiment

Figure 131 is a view for explaining the EMD system of a fourth embodiment of the present invention.

In the EMD system of the present embodiment, the content provider 301 produces for example the content file CF shown in Fig. 5A and sends this to the EMD service center 302.

Also, the content provider 301 sends the content ID of the content data, content key data Kc, electronic watermark management information (contents of the electronic watermark information to be buried in the content data and the burial position information), identifier CP\_ID of the content provider 301, identifier SP\_ID of the service provider 310 providing the content data, and the suggested retailer's price SRP of the content data to the EMD service center 302, and the key file KF shown in Fig. 5B is produced in the EMD service center 302.

Also, the EMD service center 302 stores the content file CF in the database 802a, attaches the global unique content IDs to individual content files CF, and centrally manages them. Also, the EMD service center 302 stores the produced key file KF in the KF database 153a and

centrally manages it by using the content ID.

Also, in the EMD service center 302, the secure container 806 storing the content file CF read out from the CF database 802a and the key file KF read out from the KF database 153a is produced, and the secure container 806 is stored in the secure container database.

Thereafter, the secure container database is accessed by the service provider 310 and the secure container 806 is supplied to the service provider 310.

Next, the service provider 310 produces a secure container 807 storing the content file CF and key file KF stored in the secure container 806 and the price tag data 312 indicating the sales price of the content data.

Then, the service provider 310 distributes the secure container 807 to the user home network 303 by using a predetermined communication protocol in a format not depending upon the related communication protocol or by storing the same in a storage medium.

In the user home network 303, in the case of on-line, the secure container 807 is provided to the SAM 305<sub>1</sub> etc. via the CA module 311, in the SAM 305<sub>1</sub> etc., the content key data Kc and usage control policy data 106 etc. stored in the key file KF are decrypted by using the distribution use key data KD<sub>1</sub> to KD<sub>3</sub>, and the handling such as the purchase form of the content data stored in

the content file CF is determined based on the decrypted usage control policy data 106.

Also, in the SAM 305<sub>1</sub>, etc., the usage log data 308 indicating the purchase log etc. of the content data is produced, and the usage log data 308 is transmitted to the EMD service center 302.

Also, where the secure container 807 is distributed from the SAM 305<sub>2</sub> of the user home network 303 to the SAM 305<sub>12</sub> of the user home network 303a, processing similar to that of the SAM 305<sub>2</sub> is carried out in the SAM 305<sub>12</sub>, and the usage log data 308 is transmitted from the SAM 305<sub>12</sub> to the EMD service center 302.

Note that, the processings with respect to the secure container 807 in the user home networks 303 and 303a are the same as the processings in the user home networks 103 and 303 in the first embodiment and second embodiment mentioned above.

Also, in the example shown in Fig. 131, the case where the secure container storing the content file CF and the key file KF was transmitted from the EMD service center 302 to the service provider 310 and from the service provider 310 to the user home network 303 (the case of in-band) was exemplified, but it is also possible to separately transmit the content file CF and the key file KF by the same route (the case of out-of-band).

Also, as shown in Fig. 132, it is also possible if the content file CF is supplied from the EMD service center 302 to the service provider 310, the service provider 310 supplies the content file CF to the user home network 303 and, at the same time, the key file KF produced in the EMD service center 302 is supplied from the EMD service center 302 to the SAM 305<sub>2</sub> and SAM305<sub>12</sub> of the user home networks 303 and 303a.

Fifth embodiment

Figure 133 is a view for explaining the EMD system of a fifth embodiment of the present invention.

In the EMD system of the present embodiment, the content provider 301 produces for example the content file CF shown in Fig. 5A.

Also, the content provider 301 sends the content ID of the content data, content key data Kc, electronic watermark management information (contents of the electronic watermark information to be buried in the content data and the burial position information), identifier CP\_ID of the content provider 301, identifier SP\_ID of the service provider 310 providing the content data, and the suggested retailer's price SRP of the content data to the EMD service center 302, and the key file KF shown in Fig. 5B is produced in the EMD service center 302.



The EMD service center 302 sends the produced key files KF to the content provider 301.

Also, the EMD service center 302 stores the key files KF in the KF database 153a and centrally manages  
5 the key files KF by using the content ID allocated to individual content data. At this time, the content ID is produced by for example the EMD service center 302 and globally uniquely determined for all of the content data provided by a plurality of content providers 301.

10 Next, in the content provider 301, a secure container 821 storing the produced content files CF and the key files KF received from the EMD service center 302 is produced, and the secure container 821 is stored in a common database 820.

15 In the common database 820, secure containers 821 provided by a plurality of content providers 301 are centrally managed by using the content ID.

The service provider 310 browses (searches through) the common database 820 by using for example the content  
20 ID, receives the intended secure container 821 from the common database 820, produces a secure container 822 obtained by further storing the price tag data 312 indicating the sales price of the content etc. in the secure container 821, and distributes the secure  
25 container 822 to the user home network 303.

In the user home network 303, the secure container 822 is provided to the SAM 305<sub>1</sub> etc. via the CA module 311 in the case of on-line, in the SAM 305<sub>1</sub> etc., the content key data Kc and the usage control policy data 106 etc. stored in the key files KF are decrypted by using the distribution use key data KD<sub>1</sub> to KD<sub>3</sub> or the like, and the handling such as the purchase form of the content data stored in the content files CF is determined based on the decrypted usage control policy data 106.

Also, in the SAM 305<sub>1</sub>, etc., the usage log data 308 indicating the purchase log etc. of the content data is produced, and the usage log data 308 is transmitted to the EMD service center 302.

Also, where the secure container 822 is distributed from the SAM 305<sub>2</sub> of the user home network 303 to the SAM 305<sub>12</sub> of the user home network 303a, processing similar to that in the SAM 305<sub>2</sub> is carried out in the SAM 305<sub>12</sub>, and the usage log data 308 is transmitted from the SAM 305<sub>12</sub> to the EMD service center 302.

Note that, the processings with respect to the secure container 807 in the user home networks 303 and 303a are the same as the processings in the user home networks 103 and 303 in the above first embodiment and the second embodiment.

Also, in the example shown in Fig. 133, the case

where the secure containers storing the content files CF and the key files KF were sent from the content provider 301 to the common database 820, from the common database 820 to the service provider 310, and from the service  
5 provider 310 to the user home network 303 (the case of in-band) was exemplified, but it is also possible to separately transmit the content files CF and the key files KF by the same route (the case of out-of-band).

Also, as shown in Fig. 134, it is also possible if  
10 the content files CF are stored in the common database 820 from the content providers 301, the service provider 310 obtains the content files CF from the common database 820 and, at the same time, the key files KF are sent from the EMD service center 302 to the service provider 310.  
15 In this case, the service provider 310 produces the secure container 822 by storing the content files CF obtained from the common database 820, the key files KF obtained from the EMD service center 302, and the price tag data 312.

20 The common database 820 centrally manages the content files CF by using the content IDs globally uniquely attached to the content data provided by a plurality of content providers 301.

Also, as shown in Fig. 135, it is also possible if  
25 the key files KF produced by the EMD service center 302

are sent to the SAMs 305<sub>1</sub>, 305<sub>12</sub>, etc. of the user home networks 303 and 303a. In this case, the service provider 310 distributes the content files CF to the user home network 303.

5       The price tag data 312 may be distributed to the user home network 303 by the service provider 310 too or may be distributed to the user home networks 303 and 303a by the EMD service center 302 too.

Sixth embodiment

10       Figure 136 is a view for explaining the EMD system of a sixth embodiment of the present invention.

When compared with the EMD system shown in Fig. 133 mentioned above, the EMD system of the present embodiment is different in the characteristic features that a  
15       plurality of EMD service centers 302 are provided and that the content provider 301 performs the charge processing etc. with the corresponding EMD service centers 302, but is substantially the same in points other than that.

20       The content provider 301 produces for example the content file CF shown in Fig. 5A.

Also, the content provider 301 sends the content ID of the content data, content key data Kc, electronic watermark management information (contents of the  
25       electronic watermark information to be buried in the

content data and the burial position information),  
identifier CP\_ID of the content provider 301, identifier  
SP\_ID of the service provider 310 providing the content  
data, and the suggested retailer's price SRP of the  
5 content data to one EMD service center 302 selected by  
itself (or determined in advance) among a plurality of  
EMD service centers 302, and the key file KF shown in  
Fig. 5B is produced in the EMD service center 302.

Also, the EMD service center 302 sends the produced  
10 key files KF to the corresponding content provider 301.

Also, the EMD service center 302 stores the key  
files KF in the KF database 153a and centrally manages  
the key files KF by using the content IDs allocated to  
individual content data. At this time, the content IDs  
15 are produced by for example the EMD service center 302  
and globally uniquely determined for the content data  
corresponding to all secure containers 831 stored in the  
common database 830.

Next, in the content provider 301, a secure  
20 container 831 storing the produced content files CF and  
the key files KF received from the EMD service center 302  
is produced, and the secure container 831 is stored in a  
common database 820.

In the common database 830, secure containers 831  
25 provided by a plurality of content providers 301 are

centrally managed by using the content IDs.

The service provider 310 browses (searches through) the common database 820 by using for example the content ID, receives the intended secure container 831 from the  
5 common database 820, produces a secure container 832 obtained by further storing for example the price tag data 312 indicating the sales price of the content in the secure container 831, and distributes the secure container 832 to the user home network 303.

10 In the user home network 303, the secure container 832 is provided to the SAM 305<sub>1</sub>, etc. via the CA module 311 in the case of on-line, in the SAM 305<sub>1</sub>, etc., the content key data Kc and the usage control policy data 106 etc. stored in the key files KF are decrypted by using  
15 the distribution use key data KD<sub>1</sub> to KD<sub>3</sub>, or the like, and the handling such as the purchase form of the content data stored in the content files CF is determined based on the decrypted usage control policy data 106.

Also, in the SAM 305<sub>1</sub>, etc., the usage log data 308  
20 indicating the purchase log etc. of the content data is produced, and the usage log data 308 is transmitted to the EMD service center 302.

Also, where the secure container 822 is distributed from the SAM 305<sub>2</sub> of the user home network 303 to the SAM  
25 305<sub>12</sub> of the user home network 303a, processing similar

to that in the SAM 305<sub>2</sub> is carried out in the SAM 305<sub>12</sub>, and the usage log data 308 is transmitted from the SAM 305<sub>12</sub> to the EMD service center 302.

Note that, the processings with respect to the  
5 secure container 807 in the user home networks 303 and 303a are the same as the processings in the user home networks 103 and 303 in the above first embodiment and the second embodiment.

Also, in the example shown in Fig. 136, the case  
10 where the secure containers storing the content files CF and the key files KF were sent from the content provider 301 to the common database 830, from the common database 830 to the service provider 310, and from the service provider 310 to the user home network 303 (the case of  
15 in-band) was exemplified, but it is also possible to separately transmit the content files CF and the key files KF by the same route (the case of out-of-band).

Also, as shown in Fig. 137, it is also possible if  
the content files CF are stored in the common database  
20 830 from the content providers 301, the service provider 310 obtains the content files CF from the common database 830 and, at the same time, the key files KF are sent from the EMD service center 302 to the service provider 310.  
At this time, the key file KF is sent to the content  
25 provider 301 from the EMD service center 302

corresponding to the content provider 301 produced the content file CF obtained by the service provider 310.

The service provider 310 stores the content file CF obtained from the common database 830, the key file KF obtained from the EMD service center 302, and the price tag data 312 to produce the secure container 832.

The common database 830 centrally manages the content files CF by using the content IDs globally uniquely attached to the content data provided by a plurality of content providers 301.

Also, as shown in Fig. 138, it is also possible if the key files KF produced by the EMD service center 302 are sent to the SAMs 305<sub>1</sub>, 305<sub>12</sub>, etc. of the user home networks 303 and 303a. Also at this time, the key files KF are sent to the SAMs 305<sub>1</sub>, 305<sub>12</sub>, etc. from the EMD service center 302 corresponding to the content providers 301 preparing the content files CF provided to the SAM 305<sub>1</sub>, 305<sub>12</sub>, etc.

Also, the service provider 310 distributes the content files CF to the user home network 303. The price tag data 312 may be distributed by the service provider 310 to the user home network 303 too or may be distributed by the EMD service center 302 to the user home networks 303 and 303a.

Seventh embodiment



Figure 139 is a view for explaining the EMD system of a seventh embodiment of the present invention.

The EMD system of the present embodiment is different when compared with the EMD system shown in Fig. 136 mentioned above in the point that the master source S111 of the content data is sent from the content provider 301 to the EMD service center 302 and the content file CF is produced in the EMD service center 302. The points other than that are substantially the same.

The content provider 301 sends the master source S111 of the content data to one EMD service center 302 selected by itself (or determined in advance) among a plurality of EMD service centers 302, and the content file CF shown in Fig. 5A is produced in the EMD service center 302.

The EMD service center 302 sends the produced content file CF to the corresponding content provider 301.

Also, the content provider 301 sends the content ID of the content data, content key data Kc, electronic watermark management information (contents of the electronic watermark information buried in the content data), identifier CP\_ID of the content provider 301, identifier SP\_ID of the service provider 310 providing

the content data, and the suggested retailer's price data SRP of the content data to the above one corresponding EMD service center 302, and the key file KF shown in Fig. 5B is produced in the EMD service center 302.

5       The EMD service center 302 sends the produced key file KF to the corresponding content provider 301.

Also, the EMD service center 302 stores the content files CF in the CF database 802a, stores the key files KF in the KF database 153a, and centrally manages the  
10   content files CF and the key files KF by using the content IDs allocated to the individual content data. At this time, the content IDs are produced by for example the EMD service center 302 and globally uniquely determined for the content data corresponding to all  
15   secure containers 831 stored in the common database 840.

Next, in the content provider 301, a secure container 841 storing the content file CF and the key file KF received from the corresponding EMD service center 302 is produced, and the secure container 841 is  
20   stored in the common database 840.

In the common database 840, secure containers 841 provided by a plurality of content providers 301 are centrally managed by using the content ID.

The service provider 310 browses (searches through)  
25   the common database 840 by using for example the content

ID, receives the intended secure container 841 from the common database 840, produces a secure container 842 obtained by further storing for example the price tag data 312 indicating the sales price of the content in the secure container 841, and distributes the secure container 842 to the user home network 303.

In the user home network 303, the secure container 842 is provided to the SAM 305<sub>1</sub> etc. via the CA module 311 in the case of on-line, in the SAM 305<sub>1</sub> etc., the content key data Kc and the usage control policy data 106 etc. stored in the key files KF are decrypted by using the distribution use key data KD<sub>1</sub> to KD<sub>3</sub> or the like, and the handling such as the purchase form of the content data stored in the content files CF is determined based on the decrypted usage control policy data 106.

Also, in the SAM 305<sub>1</sub> etc., the usage log data 308 indicating the purchase log etc. of the content data is produced, and the usage log data 308 is transmitted to the EMD service center 302.

Also, where the secure container 822 is distributed from the SAM 305<sub>2</sub> of the user home network 303 to the SAM 305<sub>12</sub> of the user home network 303a, processing similar to that in the SAM 305<sub>2</sub> is carried out in the SAM 305<sub>12</sub>, and the usage log data 308 is transmitted from the SAM 305<sub>12</sub> to the EMD service center 302.

Note that, the processings with respect to the secure container 807 in the user home networks 303 and 303a are the same as the processings in the user home networks 103 and 303 in the above first embodiment and  
5 the second embodiment.

Also, in the example shown in Fig. 139, the case where the secure containers storing the content files CF and the key files KF were sent from the content provider 301 to the common database 840, from the common database  
10 840 to the service provider 310, and from the service provider 310 to the user home network 303 (the case of in-band) was exemplified, but it is also possible to separately transmit the content files CF and the key files KF by the same route (the case of out-of-band).

15 Also, as shown in Fig. 140, it is also possible if the content files CF are stored in the common database 830 from the content providers 301, the service provider 310 obtains the content files CF from the common database 840 and, at the same time, the key files KF are sent from  
20 the EMD service center 302 to the service provider 310. At this time, the key files KF are sent to the content provider 301 from the EMD service center 302 corresponding to the content providers 301 preparing the content files CF obtained by the service provider 310.

25 The service provider 310 stores the content file CF

obtained from the common database 840, the key file KF obtained from the EMD service center 302, and the price tag data 312 to produce the secure container 842.

5 The common database 830 centrally manages the content files CF by using the content IDs globally uniquely attached to the content data provided by a plurality of content providers 301.

Also, as shown in Fig. 141, it is also possible if the key files KF produced by the EMD service center 302 are sent to the SAMs 305<sub>1</sub>, 305<sub>12</sub>, etc. of the user home networks 303 and 303a. Also at this time, the key files KF are sent to the SAMs 305<sub>1</sub>, 305<sub>12</sub>, etc. from the EMD service center 302 corresponding to the content providers 301 preparing the content files CF provided to the SAMs 305<sub>1</sub>, 305<sub>12</sub>, etc.

Also, the service provider 310 distributes the content files CF to the user home network 303. The price tag data 312 may be distributed by the service provider 310 to the user home network 303 too or may be distributed by the EMD service center 302 to the user home networks 303 and 303a.

#### Eighth embodiment

Figure 142 is a view for explaining the EMD system of an eighth embodiment of the present invention.

25 In the EMD system of the present embodiment, for

example, the content file CF shown in Fig. 5A produced by the EMD service center 302 by using the master source provided from the content provider 301 to the EMD service center 302 or the content file CF shown in Fig. 5A produced by the content provider 301 and provided to the EMD service center 302 and the key file KF shown in Fig. 5B produced by the EMD service center 302 are distributed by the EMD service center 302 via the service provider 310 or directly to the SAM 305<sub>1</sub> of the user home network 303.

Here, the service provider 310 sends the price tag data 312 indicating the sales price of the content file CF to the user home network 303 and, at the same time, registers and authenticates the price tag data 312 in the EMD service center 302.

Also, the service provider 310 registers itself in the EMD service center 302 as the distribution business.

In the EMD system of the present embodiment, for example, the SAM 305<sub>1</sub> of the user home network 303 becomes the distribution business for distributing the content files CF and key files KF obtained from the service provider 310 or the EMD service center 302 to the SAM 305<sub>2</sub> in the user home network 303 and/or SAM 305<sub>12</sub> etc. in the user home network 303a.

Note, in this case, for example, the EMD service

center 302 prohibits selling (redistributing) the purchased content data C while adding a certain sales margin to obtain a profit after the SAM 305<sub>1</sub> purchases the content data C stored in the content file CF.

5           In the EMD system of the present embodiment, it is permitted to the SAM 305<sub>1</sub> to copy the content data C to another SAM under the condition that content data for which the purchase form is not determined or content data C for which reproduction charge is determined as the  
10 purchase form is redistributed without a sale profit margin. Note that, this will be referred to as inter-apparatus redistribution.

          Also, in the EMD system of the present embodiment, inter-apparatus trade in a form without a sale profit  
15 margin is permitted for a content file CF (or secure container) distributed from the service provider 310 to the SAM 305<sub>1</sub>.

          Also, in the present embodiment, where the SAM 305<sub>1</sub> performs sells (distributes) the content data C in a form  
20 taking a sales profit margin, the SAM 305<sub>1</sub> registers itself in the EMD service center 302 as distribution business and receives permission and, at the same time, registers the price tag data 312 indicating the sales price of the content data C in the EMD service center  
25 302. Then, it directly receives the content file CF and

the key file KF from the CF database 802a and the KF database 153a in the EMD service center 302 not via the service provider 310.

Ninth embodiment

5        Figure 143 is a view for explaining the EMD system of a ninth embodiment of the present invention.

10        In the EMD system of the present embodiment, the characteristic feature resides in that each of the content providers 301 functions as an EMD service center 302 in addition functioning as a content provider.

      In this case, where there are a plurality of content providers, each content provider 301 functions as an EMD service center 302.

15        A content provider 301 distributes a secure container 851 storing the content file CF and the key file KF to the service provider 310.

20        The service provider 310 further adds the price tag data 312 to the content file CF and the key file KF stored by the secure container 851 to produce a secure container 852 and distributes this to the user home network 303.

25        In the user home networks 303 and 303a, the purchase form etc. of the content file CF are determined based on the usage control policy data 106 stored in the key file KF, the usage log data 308 in accordance with that is



produced, and this is transmitted to the EMD service center 302 in the content provider 301.

At this time, the usage log data 308 is produced for every content provider 301.

5       The EMD service center 302 of the content provider 301 distributes the profit paid by the users of the SAMs 305<sub>1</sub> and 305<sub>12</sub> with the corresponding service provider 310 based on the usage log data 308.

10       Also, the log data concerning the distribution service is sent from the CA module 311 of the user home network 303 to the corresponding service provider 310, whereby the charge processing with respect to the distribution service is carried out in the service provider 310.

15       The present invention is not limited to the above embodiments.

20       In the above embodiments, the case where audio data was used as the content data was exemplified, but it is also possible to use video data, audio and/or video data, text data, and a computer program or the like as the content data.

25       Also, in the above embodiments, the case where the key files KF were produced in the EMD service centers 102 and 302 was exemplified, but it is also possible to produce the key files KF in the content providers 101 and

301.

In this case, the format of the key file KF corresponding to Fig. 7 becomes as shown in Fig. 144. As shown in Fig. 144, the related key file KF has basically  
5 the same information as the key file KF shown in Fig. 7 except that signature data produced by using the secret key data  $K_{CP,S}$  of the content providers 101 and 301 are used.

Also, in the above embodiments, the case where the  
10 usage control status data 166 is transmitted from the user home networks 103 and 303 to the EMD service centers 102 and 302 in real time was exemplified, but it is also possible if the usage control status data 166 is transmitted to the content providers 101 and 301 and/or  
15 service provider 310. By this, the content providers 101 and 301 and the service provider 310 can quickly grasp the purchase situation of the contents provided and distributed by themselves and can reflect the same in their service thereafter.

20 Below, effects by the EMD system of the above embodiments will be explained again while mentioning the related art and the problems thereof.

With the ROM type storage media which had been used as the means for distributing digital content (content  
25 data) in the days when digital broadcasts (data

broadcasts) and the Internet and other digital networks were not so developed, the digital content was stored and distributed in an unencrypted state. In the days when the digital network was not so developed, it was enough to consider methods for preventing casual copying by users on the user home network for the protection of the copyrights of these contents.

In recent days where the digital network has been developed, however, since ROM type storage media carrying unencrypted content can be obtained by general citizens anytime and everywhere, any individual can purchase one and easily compress and upload the data on the network. Particularly, the Internet is a network connecting the entire world. Therefore, it becomes possible to freely upload the unencrypted content on the Internet and for people to download it on their own personal terminals. Accordingly, there has arisen a possibility of serious infringement of the copyrights of the owners of the content (content providers).

Further, it also becomes possible for people not to upload the content in the unencrypted state, but to bury electronic watermark information of their own in that content, encrypt the data, and charge for the data on their own and thereby deliberately sell the digital content on the Internet behind the scenes without the

permission of the copyright owner. At this time, since a share of the sales is not returned to the owner of the content, the copyright of the owner of the content (content providers) will be seriously infringed.

5       Also, by getting the permission of the copyright owner and concluding a contract for returning part of the sales to the owner of content (content provider) in advance, it becomes possible to offer a distribution service capable of generating profit by distributing the  
10   digital content, but basically the content provider does not favor circulation by such a secondary usage of content. Rental, secondhand sale, etc. are other types of business by secondary usage of the content.

          When a distribution service by secondary usage  
15   appears, the problem of infringement of copyrights is sure to occur, so a long time is taken for setting up the service in the right direction. The distribution service ends up being first started without establishing a contract with the content provider. After the problem of  
20   infringement of copyrights occurs, the distribution of profit to the owners and protection of the copyrights start to be considered and permission as the distribution service is obtained. The rental CD and the rental video businesses correspond to this. The secondhand sale of  
25   game software etc. is a serious problem. In the

secondhand sale of game software, part of the profit from the sales is not returned to the owners of the content. The owners have brought court actions against this, but these have been dismissed. This is very hard on the owners. Secondhand game software is sold in large volumes with a price of half or less of new software, therefore the market is very attractive for the users and a large influence is exerted upon the sale of new software.

Secondary usage of content means when a user who purchases a ROM type storage medium on which digital content has been already stored by the owner of the content using the ROM type storage medium distributed as a circulating means to obtain a profit further circulates the product. The fact that the purchasing user obtains a profit is not considered desirable from the standpoint of the (content provider) owner even if part of the profit is returned to it. With movie content etc., the owner of the content is protected by law in the form of recording rights/distribution rights. When purchasing content which an owner circulates in the public, the assumption is that it not be circulated further from the purchasing user. Groups of owners of game software have raised suits at courts to suppress secondary usage businesses attempting to apply such distribution right to game software as well.

Owners of content want to get distributors distributing digital content which they hold copyrights to under their control (they would like to know to whom the content is being distributed to). When there is a distributor desiring to distribute digital content to which one holds a copyright so as to provide a distribution service and make a profit, a system is desirable by which the owner of the content can directly supply the digital content.

Note that the distributor spoken of here designates a business that obtains a profit by collecting the profit margin of a few percent with respect to the price of the digital content.

A case where a profit margin is collected when delivering digital content to another apparatus/storage medium is defined as a content trade session distribution service, while a case where a profit margin is not collected is defined as inter-apparatus redistribution. The latter is legal under the principle of supra-distribution.

In the current system for management of distribution of digital content over the network where the service provider authors the content of its own distribution service from a ROM type storage medium storing unencrypted content circulated by the content provider

for a distribution service, when considering the situation where one digital content owned by the content provider is distributed by a plurality of service providers, irrespective of the fact that it is identical content, authoring is carried out so that the rights are cleared by a CA module/electronic settlement tool employed by each service provider. Therefore, the formats of the encryption key (content key data) to be used and the licensing conditions of the content (usage control policy data) are different according to each service provider, so common rights clearing rules cannot be provided on the user home network. In such a case, by settling up for all of the key data used by the CA modules/electronic settlement tools by the CA modules/electronic settlement tools of the network apparatuses and then following the SCMS rules, common rights clearing rules can be realized on the user home network.

Also, even if the content encrypted by the key of a CA module/electronic settlement tool and the key data are passed through the network apparatus as they are and stored on a storage medium of the storage apparatus via the user home network bus (IEEE1394 or the like) and the purchase and settlement processing of the content can be performed remotely through the network apparatus from an

apparatus connected to the 1394 bus, since there is a descrambler for decrypting the encrypted content in the network apparatus, in the end, reproduction cannot be carried out unless the content and the key data are returned back to the network apparatus at the time of reproduction (network CA).

As explained above, the existence of the ROM type storage medium storing unencrypted content, which has been widely circulated in the world up to the present, is at the root of the problem for current digital content network distribution services. This is a system where the form of the digital content can be produced by a person other than the content provider and where a person selling the content to a user can obtain payment for it. Therefore, the profit of the content provider is illegitimately infringed by secondary usage of the content. Also, the distribution of the authored digital content is not strictly managed by the content provider, therefore it is difficult to monitor all profits earned by the digital content which it holds a copyright to and if its share of the profits is being returned to it.

The EMD system of the embodiments explained above solves the conventional problems mentioned above.

Namely, in the EMD system of the present embodiment, the digital contents authored by the content provider are



all managed in a database on the content provider side by preparing content format and usage control policy data on the content provider side. The usage control policy data of the content is further authenticated and registered in  
5 the EMD service center (clearinghouse) as a third party reliable authority manager.

By doing this, the interested parties of the content provider can place the rights clearing rules of the digital content completely under their control and manage  
10 the distribution channels at the content provider side. Also, in the present case, steps are taken so that a distributor interposed between the user cannot see the content of the data of the usage control policy produced at the content provider side.

15 Also, in the EMD system of the present embodiment, the ROM type storage medium is considered as one means of distribution and the existence of the digital content stored there is freed from the ROM type storage medium. A content format having value of existence by solely  
20 digital content without regard as to means of distribution and channels of distribution is proposed. The digital content is managed in a certain prescribed format on the content provider side. Therefore, by considering the mounting of the digital content of that  
25 format in a ROM type storage medium, whether the content

is circulated as a ROM type storage medium or circulated over a digital network, it becomes possible to provide common rights clearing rules for ROM -> RAM and for network -> RAM on the user home network. This is provided so that sale sessions of the digital content are all defined and managed by the content provider. Due to this, common rights clearing not depending on the means of distribution or the channel of distribution becomes possible. Also, by stipulating this format of content defined at the content provider side as the minimum unit for trading the digital content, common rights clearing rules can be provided without regard as to the type of the content format used in the subsequent distribution process. By returning the charge information produced at the time of purchase at the user home network not to the service provider, but to the EMD service center as a third party reliable authority manager and returning it therefrom to the service provider, the problems of the business of secondary usage of content were solved.

As explained above, according to the present invention, it becomes possible to handling data in the data processing device of the content data provided by the data providing apparatus based on the usage control policy data of the data providing apparatus.

As a result, it becomes possible to suitably protect

profit according to the content data by the interested party of the data providing apparatus and, at the same time, the load of the inspection by the related interested party can be reduced.

2025-09-23 14:00:00

CLAIMS

1. A data providing system for distributing  
content data from a data providing apparatus to a data  
processing apparatus and managing said data providing  
5 apparatus and said data processing apparatus by a  
management apparatus, wherein

said management apparatus prepares a key file  
storing encrypted content key data and encrypted usage  
control policy data indicating handling of said content  
10 data,

said data providing apparatus provides said  
content data encrypted by using said content key data,  
and

said data processing apparatus decrypts said  
15 content key data and said usage control policy data  
stored in said key file and determines the handling of  
said content data based on the related decrypted usage  
control policy data.

2. A data providing system as set forth in claim  
20 1, wherein said management apparatus adds signature data  
for verification of the legitimacy of the producer of the  
key file to the key file.

3. A data providing system as set forth in claim  
1, wherein said data providing apparatus prepares a  
25 content file storing the content data and provides the

content file to the data processing apparatus.

4. A data providing system as set forth in claim  
3, wherein said data providing apparatus adds signature  
data for verification of the legitimacy of the producer  
5 of the content file to the content file.

5. A data providing system as set forth in claim  
1, wherein

the data providing apparatus prepares usage  
control policy data and sends it to said management  
10 apparatus,

said data processing apparatus determines at  
least one of the purchase form and the usage form of the  
distributed content data based on the usage control  
policy data and sends log data showing the log of at  
15 least one of the purchase form and usage form decided to  
said management apparatus, and

said management apparatus performs profit  
distribution processing for distributing the profit  
obtained along with the purchase and usage of the content  
20 data in the data processing apparatus to the interested  
parties of the data providing apparatus based on the  
received log data.

6. A data providing system for distributing  
content data from a data providing apparatus to a data  
25 processing apparatus and managing said data providing

apparatus and said data processing apparatus by a management apparatus, wherein

said management apparatus prepares a key file storing encrypted content key data and encrypted usage control policy data indicating handling of said content data,

said data providing apparatus distributes a module storing a content file storing the content data encrypted by using said content key data and said key file received from said management apparatus to said data processing apparatus, and

said data processing apparatus decrypts said content key data and said usage control policy data stored in said distributed module and determines the handling of said content data based on the related decrypted usage control policy data.

7. A data providing system as set forth in claim 6, wherein said management apparatus generates signature data for verifying the legitimacy of the producer of the key file and prepares the key file further storing that signature data.

8. A data providing system as set forth in claim 6, wherein

the data providing apparatus generates said content key data and usage control policy data and sends

them to said management apparatus and

said management apparatus prepares said key file based on said received content key data and usage control policy data and registers the prepared key file.

5           9. A data providing system as set forth in claim 7, wherein said data providing apparatus prepares signature data for verifying at least one of the legitimacy of a producer and distributor of the content key file and the distributor of the key file and  
10 distributes said module further storing the signature data to said data processing apparatus.

10. A data providing system as set forth in claim 9, wherein said data processing apparatus verifies the signature data stored in the module to verify at least  
15 one of the legitimacy of a producer and distributor of the content file and a producer and distributor of the key file.

11. A data providing system as set forth in claim 6, wherein said management apparatus  
20 prepares said key file storing said content key file and said usage control policy data encrypted using distribution use key data and  
distributes said distribution use key data to said data processing apparatus.

25           12. A data providing system as set forth in claim

6, wherein said management apparatus and said data processing apparatus comprise a plurality of distribution use key data of defined periods of validity and use distribution use key data of corresponding periods.

5           13. A data providing system as set forth in claim 11, wherein

                  said data providing apparatus prepares signature data using its own secret key data and

                  said data processing apparatus verifies the  
10   legitimacy of the signature data using public key data corresponding to said secret key data.

                  14. A data providing system for distributing content data from a data providing apparatus to a data processing apparatus and managing said data providing  
15   apparatus and said data processing apparatus by a management apparatus, wherein

                  said management apparatus prepares a key file storing encrypted content key data and encrypted usage control policy data indicating handling of said content  
20   data,

                  said data providing apparatus distributes a module storing a content file containing content data encrypted by using said content key data and the key file received from said management apparatus to said data  
25   processing apparatus, and



said data processing apparatus decrypts said content key data and said usage control policy data stored in said distributed module and determines the handling of said content data based on the related  
5 decrypted usage control policy data.

15. A data providing system for distributing content data from a data providing apparatus to a data processing apparatus and managing said data providing apparatus and said data processing apparatus by a  
10 management apparatus, wherein

said management apparatus prepares a key file storing encrypted content key data and encrypted usage control policy data indicating handling of said content data,

15 said data providing apparatus individually distributes the content file storing the content data encrypted by using said content key data and said key file received from said management apparatus to said data processing apparatus, and

20 said data processing apparatus decrypts said content key data and said usage control policy data stored in said distributed key file and determines the handling of the content data stored in said distributed content file based on the related decrypted usage control  
25 policy data.

16. A data providing system for distributing content data from a data providing apparatus to a data processing apparatus and managing said data providing apparatus and said data processing apparatus by a

5 management apparatus, wherein

said management apparatus prepares a key file storing encrypted content key data and encrypted usage control policy data indicating handling of said content data and distributes the related prepared key file to  
10 said data processing apparatus,

said data providing apparatus distributes a content file storing the content data encrypted by using said content key data to said data processing apparatus, and

15 said data processing apparatus decrypts said content key data and said usage control policy data stored in said distributed key file and determines the handling of the content data stored in said distributed content file based on the related decrypted usage control  
20 policy data.

17. A data providing system for distributing content data from a data providing apparatus to a data processing apparatus and managing said data providing apparatus and said data processing apparatus by a

25 management apparatus, wherein

said management apparatus prepares a key file storing encrypted content key data and encrypted usage control policy data indicating handling of said content data,

5           said data providing apparatus distributes a module storing the content data encrypted by using said content key data and said key file received from said management apparatus to said data processing apparatus, and

10           said data processing apparatus decrypts said content key data and said usage control policy data stored in said distributed module and determines the handling of said content data based on the related decrypted usage control policy data.

15           18. A data providing system for distributing content data from a data providing apparatus to a data processing apparatus and managing said data providing apparatus and said data processing apparatus by a management apparatus, wherein

20           said management apparatus prepares a key file storing encrypted content key data and encrypted usage control policy data indicating handling of said content data,

            said data providing apparatus individually  
25   distributes the content data encrypted by using said

content key data and said key file received from said management apparatus to said data processing apparatus, and

5       said data processing apparatus decrypts said content key data and said usage control policy data stored in said distributed key file and determines the handling of said distributed content data based on the related decrypted usage control policy data.

19. A data providing system for distributing  
10       content data from a data providing apparatus to a data processing apparatus and managing said data providing apparatus and said data processing apparatus by a management apparatus, wherein

15       said management apparatus prepares a key file storing encrypted content key data and encrypted usage control policy data indicating handling of said content data and distributes the related prepared key file to said data processing apparatus,

20       said data processing apparatus distributes the content data encrypted by using said content key data to said data processing apparatus, and

25       said data processing apparatus decrypts said content key data and said usage control policy data stored in said distributed key file and determines the handling of said distributed content data based on the

related decrypted usage control policy data.

20. A data providing system for distributing  
content data from a data providing apparatus to a data  
processing apparatus and managing said data providing  
5 apparatus and said data processing apparatus by a  
management apparatus, wherein

said management apparatus prepares encrypted  
content key data and encrypted usage control policy data  
indicating handling of said content data,  
10 said data providing apparatus individually  
distributes the content data encrypted by using said  
content key data, said encrypted content key data  
received from said management apparatus, and said  
encrypted usage control policy data to said data  
15 processing apparatus, and

said data processing apparatus decrypts said  
distributed content key data and said usage control  
policy data and determines the handling of the content  
data stored in said distributed content file based on the  
20 related decrypted usage control policy data.

21. A data providing system for distributing  
content data from a data providing apparatus to a data  
processing apparatus and managing said data providing  
apparatus and said data processing apparatus by a  
25 management apparatus, wherein

said management apparatus prepares encrypted content key data and encrypted usage control policy data indicating handling of said content data and distributes the same to said data processing apparatus,

5           said data providing apparatus distributes the content data encrypted by using said content key data to said data processing apparatus, and

          said data processing apparatus decrypts said distributed content key data and said usage control  
10 policy data and determines the handling of said distributed content data based on the related decrypted usage control policy data.

22. A data providing system comprising a data providing apparatus, a data distribution apparatus, a  
15 data processing apparatus, and a management apparatus, wherein

          said management apparatus prepares a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of said  
20 content data,

          said data providing apparatus provides said content data encrypted by using said content key data,

          said data distribution apparatus distributes said provided content data to said data processing  
25 apparatus, and

said data processing apparatus decrypts said content key data and said usage control policy data stored in said key file and determines the handling of said distributed content data based on the related  
5 decrypted usage control policy data.

23. A data providing system as set forth in claim 22, wherein

said data providing apparatus provides a first module storing content data encrypted by using said  
10 content key data, said encrypted content key data, and encrypted usage control policy data showing the handling of the content data to said data distribution apparatus,  
said data distribution apparatus distributes a second module storing said encrypted content data,  
15 content key data, and usage control policy data stored in said received first module to said data processing apparatus, and

said data processing apparatus decrypts said content key data and said usage control policy data  
20 stored in said distributed second module and determines the handling of said content data based on the related decrypted usage control policy data.

24. A data providing system as set forth in claim 22, wherein said data distribution apparatus prepares a  
25 second module including said provided first module and

distributes the prepared second module to said data processing apparatus.

25. A data providing system as set forth in claim 22, wherein said data distribution apparatus distributes said second module further storing price data showing the price of the content data to said data processing apparatus.

26. A data providing system as set forth in claim 25, wherein said data distribution apparatus determines the price data based on a wholesale price determined for said content data by said data providing apparatus.

27. A data providing system as set forth in claim 22, wherein said data providing apparatus provides a first module further storing signature data for verifying the legitimacy of a producer and transmitter of at least one data of the content data, content key data, and usage control policy data to said data distribution apparatus.

28. A data providing system as set forth in claim 22, wherein said data distribution apparatus provides said second module further storing signature data for verifying the legitimacy of a producer and transmitter of at least one data among the content data, content key data, and usage control policy data to said data processing apparatus.

29. A data providing system as set forth in claim



22, wherein

said data processing apparatus determines at least one of the purchase form and the usage form of the distributed content data based on the usage control policy data and sends log data showing the log of at least one of the purchase form and usage form decided to said management apparatus and

said management apparatus performs profit distribution processing for distributing the profit obtained along with the purchase and usage of the content data in the data processing apparatus to the interested parties of the data providing apparatus and data distribution apparatus based on the received log data.

30. A data providing system as set forth in claim 22, wherein

said data processing apparatus sends distribution use log data relating to the distribution of the data distribution apparatus to said data distribution apparatus and

said data distribution apparatus performs charge processing relating to that distribution based on the distribution use log data.

31. A data providing system for providing content data from a data providing apparatus to a data distribution apparatus, distributing the content data

from said data distribution apparatus to a data processing apparatus, and managing said data providing apparatus, said data distribution apparatus, and said data processing apparatus by a management apparatus,

5 wherein

said management apparatus prepares a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of said content data,

10 said data providing apparatus provides a first module storing a content file storing the content data encrypted by using said content key data and said key file received from said management apparatus to said data distribution apparatus,

15 said data distribution apparatus distributes a second module storing said provided content file and said key file to said data processing apparatus, and

said data processing apparatus decrypts said content key data and said usage control policy data stored in said distributed second module and determines the handling of said content data stored in said distributed second module based on the related decrypted usage control policy data.

20 32. A data providing system as set forth in claim 25 31, wherein

said data providing apparatus produces said content key data and said usage control policy data and sends them to said management apparatus and

said management apparatus produces said key  
5 file based on said received content key data and usage control policy data and registers said received content key data and usage control policy data.

33. A data providing system as set forth in claim 31, wherein said data providing apparatus prepares  
10 signature data for verifying at least one of the legitimacy of a producer and distributor of the content key file and the distributor of the key file and distributes said first module further storing the signature data to said data processing apparatus.

15 34. A data providing system as set forth in claim 31, wherein said data providing apparatus prepares signature data for verifying at least one of the legitimacy of a producer and distributor of the content key file and the distributor of the key file and  
20 distributes said second module further storing the signature data to said data processing apparatus.

35. A data providing system as set forth in claim 33, wherein

said data providing apparatus prepares  
25 signature data using its own secret key data and

said data processing apparatus verifies the legitimacy of the signature data using public key data corresponding to said secret key data.

36. A data providing system as set forth in claim  
5 33, wherein

said data providing apparatus distributes said module further storing public key certificate data for certifying the legitimacy of the public key data to said data processing apparatus and

10 said data processing apparatus verifies the signature data using the public key data stored in the distributed public key certificate data.

37. A data providing system as set forth in claim  
36, wherein

15 said management apparatus distributes public key certificate data for certifying the legitimacy of the public key data to said data processing apparatus and

said data processing apparatus verifies the signature data using the public key data stored in the  
20 distributed public key certificate data.

38. A data providing system as set forth in claim  
33, wherein

said data distribution apparatus prepares said signature data using its own secret key data and

25 said data processing apparatus verifies the

legitimacy of the signature data using public key data corresponding to said secret key data.

39. A data providing system as set forth in claim 38, wherein

5           said data distribution apparatus distributes said module further storing public key certificate data for certifying the legitimacy of the public key data to said data processing apparatus and

10           said data processing apparatus verifies the signature data using the public key data stored in the distributed public key certificate data.

40. A data providing system as set forth in claim 38, wherein

15           said management apparatus distributes said public key certificate data for certifying the legitimacy of the public key data to said data processing apparatus and

20           said data processing apparatus verifies the signature data using the public key data stored in the distributed public key certificate data.

41. A data providing system as set forth in claim 31, wherein

25           said data processing apparatus determines at least one of the purchase form and the usage form of the distributed content data based on the usage control

policy data and sends log data showing the log of at least one of the purchase form and usage form decided to said management apparatus, and

5           said management apparatus performs profit distribution processing for distributing the profit obtained along with the purchase and usage of the content data in the data processing apparatus to the interested parties of the data providing apparatus and the data distribution apparatus based on the received log data.

10           42. A data providing system as set forth in claim 31, wherein said data distribution apparatus distributes said second module further storing price data showing the price of the content data to said data processing apparatus.

15           43. A data providing system as set forth in claim 42, wherein said management apparatus registers the price data received from said data distribution device.

20           44. A data providing system as set forth in claim 31, wherein said data processing apparatus comprises a module giving resistance to outside monitoring and tampering of the processing content, predetermined data stored in an internal memory, and data being processed.

25           45. A data providing system for providing content data from a data providing apparatus to a data distribution apparatus, distributing the content data

from said data distribution apparatus to a data processing apparatus, and managing said data providing apparatus, said data distribution apparatus, and said data processing apparatus by a management apparatus,

5 wherein

said management apparatus prepares a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of said content data,

10 said data providing apparatus provides a first module storing a content file containing the content data encrypted by using said content key data and a key file received from said management apparatus to said data distribution apparatus,

15 said data distribution apparatus distributes a second module storing said provided content file to said data processing apparatus, and

said data processing apparatus decrypts said content key data and said usage control policy data  
20 stored in said distributed second module and determines the handling of said content data stored in said distributed second module based on the related decrypted usage control policy data.

46. A data providing system for providing content  
25 data from a data providing apparatus to a data

distribution apparatus, distributing the content data  
from said data distribution apparatus to a data  
processing apparatus, and managing said data providing  
apparatus, said data distribution apparatus, and said  
5 data processing apparatus by a management apparatus,  
wherein

said management apparatus prepares a key file  
storing encrypted content key data and encrypted usage  
control policy data indicating the handling of said  
10 content data,

said data providing apparatus individually  
distributes a content file storing the content data  
encrypted by using said content key data and said key  
file received from said management apparatus to said data  
15 distribution apparatus,

said data distribution apparatus individually  
distributes said distributed content file and key file to  
said data processing apparatus, and

said data processing apparatus decrypts said  
20 content key data and said usage control policy data  
stored in said distributed key file and determines the  
handling of the content data stored in said distributed  
content file based on the related decrypted usage control  
policy data.

25 47. A data providing system as set forth in claim



46, wherein said content file and said key file include data for clearing indicating their mutual correspondence.

48. A data providing system for distributing content data from a data providing apparatus to a data processing apparatus and managing said data providing apparatus and said data processing apparatus by a management apparatus, wherein

said management apparatus prepares a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of said content data and distributes the related prepared key file to said data processing apparatus,

said data providing apparatus provides a content file storing the content data encrypted by using said content key data to said data distribution apparatus,

said data distribution apparatus distributes said provided content file to said data processing apparatus, and

said data processing apparatus decrypts said content key data and said usage control policy data stored in said distributed key file and determines the handling of the content data stored in said distributed content file based on the related decrypted usage control policy data.

49. A data providing system as set forth in claim 48, wherein said content file and said key file include data for clearing indicating their mutual correspondence.

50. A data providing system for providing content  
5 data from a data providing apparatus to a data  
distribution apparatus, distributing the content data  
from said data distribution apparatus to a data  
processing apparatus, and managing said data providing  
apparatus, said data distribution apparatus, and said  
10 data processing apparatus by a management apparatus,  
wherein  
said management apparatus prepares a key file  
storing encrypted content key data and encrypted usage  
control policy data indicating the handling of said  
15 content data,  
said data providing apparatus provides a first  
module storing the content data encrypted by using said  
content key data and said key file received from said  
management apparatus to said data distribution apparatus,  
20 said data distribution apparatus distributes a  
second module storing said provided content data and said  
key file to said data processing apparatus, and  
said data processing apparatus decrypts said  
content key data and said usage control policy data  
25 stored in said distributed second module and determines

the handling of said content data stored in said distributed second module based on the related decrypted usage control policy data.

51. A data providing system for providing content  
5 data from a data providing apparatus to a data distribution apparatus, distributing the content data from said data distribution apparatus to a data processing apparatus, and managing said data providing apparatus, said data distribution apparatus, and said  
10 data processing apparatus by a management apparatus, wherein

said management apparatus prepares a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of said  
15 content data,

said data providing apparatus individually distributes the content data encrypted by using said content key data and said key file received from said management apparatus to said data distribution apparatus,

20 said data distribution apparatus individually distributes said distributed content data and said key file to said data distribution apparatus, and

said data processing apparatus decrypts said content key data and said usage control policy data  
25 stored in said distributed key file and determines the

handling of said distributed content data based on the related decrypted usage control policy data.

52. A data providing system for distributing content data from a data providing apparatus to a data processing apparatus and managing said data providing apparatus and said data processing apparatus by a management apparatus, wherein

said management apparatus prepares a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of said content data and distributes the related prepared key file to said data processing apparatus,

said data processing apparatus provides the content data encrypted by using said content key data to said data distribution apparatus,

said data distribution apparatus distributes said provided content data to said data processing apparatus, and

said data processing apparatus decrypts said content key data and said usage control policy data stored in said distributed key file and determines the handling of said distributed content data based on the related decrypted usage control policy data.

53. A data providing system for providing content data from a data providing apparatus to a data

distribution apparatus, distributing the content data  
from said data distribution apparatus to a data  
processing apparatus, and managing said data providing  
apparatus, said data distribution apparatus, and said  
5 data processing apparatus by a management apparatus,  
wherein

said management apparatus provides encrypted  
content key data and encrypted usage control policy data  
indicating the handling of said content data to said data  
10 providing apparatus,

said data providing apparatus individually  
distributes the content data encrypted by using said  
content key data and said encrypted content key data and  
said encrypted usage control policy data received from  
15 said management apparatus to said data distribution  
apparatus,

said data distribution apparatus individually  
distributes said distributed content data, said encrypted  
content key data, and said encrypted usage control policy  
20 data to said data distribution apparatus, and

said data processing apparatus decrypts said  
distributed content key data and said usage control  
policy data and determines the handling of said  
distributed content data based on the related decrypted  
25 usage control policy data.

54. A data providing system for providing content data from a data providing apparatus to a data distribution apparatus, distributing the content data from said data distribution apparatus to a data processing apparatus, and managing said data providing apparatus, said data distribution apparatus, and said data processing apparatus by a management apparatus, wherein

10       said management apparatus provides encrypted content key data and encrypted usage control policy data indicating the handling of said content data to said data processing apparatus,

15       said data providing apparatus provides the content data encrypted by using said content key data to said data distribution apparatus,

      said data distribution apparatus distributes said provided content data to said data processing apparatus, and

20       said data processing apparatus decrypts said distributed said content key data and said usage control policy data and determines the handling of said distributed content data based on the related decrypted usage control policy data.

55. A data providing apparatus, a data distribution apparatus, a management apparatus, and a data processing

apparatus, wherein

said data providing apparatus provides master  
source data of content to said management apparatus,

said management apparatus manages said data  
5 providing apparatus, said data distribution apparatus,  
and said data processing apparatus, encrypts said  
provided master source data by using content key data to  
prepare content data, prepares a content file storing the  
related content data, prepares a key file storing said  
10 encrypted content key data and encrypted usage control  
policy data indicating the handling of said content data,  
and provides said content file and said key file to said  
data distribution apparatus,

said data distribution apparatus distributes  
15 said provided content file and said key file to said data  
processing apparatus, and

said data processing apparatus decrypts said  
content key data and said usage control policy data  
stored in said distributed key file and determines the  
20 handling of the content data stored in said distributed  
content file based on the related decrypted usage control  
policy data.

56. A data providing system as set forth in claim  
55, wherein

25 said management apparatus prepares a first

module storing said content file and said key file and provides said first module to said data distribution apparatus and

5       said data distribution apparatus produces a second module storing said content file and said key file stored in said first module and distributes it to said data processing apparatus.

57. A data providing system as set forth in claim 55, wherein said management apparatus

10       comprises at least one database among a database for storing and managing said content file, a database for storing and managing said key file, and a database for storing and managing said usage control policy data and

15       centrally manages at least one among said content file, said key file, and said usage control policy data by using a content identifier uniquely allocated to said content data.

20       58. A data providing system comprising a data providing apparatus, a data distribution apparatus, a management apparatus, and a data processing apparatus, wherein

25       said data providing apparatus provides master source data of content to said management apparatus, said management apparatus manages said data



providing apparatus, said data distribution apparatus,  
and said data processing apparatus, encrypts said  
provided master source data by using content key data to  
prepare content data, prepares a content file storing the  
5 related content data, prepares a key file storing said  
encrypted content key data and encrypted usage control  
policy data indicating the handling of said content data,  
provides said content file to said data distribution  
apparatus, and provides said key file to said data  
10 processing apparatus,

said data distribution apparatus distributes  
said provided content file to said data processing  
apparatus, and

said data processing apparatus decrypts said  
15 content key data and said usage control policy data  
stored in said distributed key file and determines the  
handling of the content data stored in said distributed  
content file based on the related decrypted usage control  
policy data.

20 59. A data providing system comprising a data  
providing apparatus, a data distribution apparatus, a  
management apparatus, and a data processing apparatus,  
wherein

said data providing apparatus provides a  
25 content file storing encrypted content data using content

key data to said management apparatus,

said management apparatus manages said data providing apparatus, said data distribution apparatus, and said data processing apparatus, prepares a key file  
5 storing said encrypted content key data and encrypted usage control policy data indicating the handling of said content data, and provides said content file provided from said data providing apparatus and said prepared key file to said data distribution apparatus,

10 said data distribution apparatus distributes said provided content file and said key file to said data processing apparatus, and

said data processing apparatus decrypts said content key data and said usage control policy data  
15 stored in said distributed key file and determines the handling of the content data stored in said distributed content file based on the related decrypted usage control policy data.

60. A data providing system as set forth in claim  
20 59, wherein

said management apparatus prepares a first module storing said content file and said key file and provides said first module to said data distribution apparatus and

25 said data distribution apparatus produces a

second module storing said content file and said key file stored in said first module and distributes it to said data processing apparatus.

61. A data providing system comprising a data  
5 providing apparatus, a data distribution apparatus, a management apparatus, and a data processing apparatus, wherein

said data providing apparatus provides a content file storing encrypted content data using content  
10 key data to said management apparatus,

said management apparatus manages said data providing apparatus, said data distribution apparatus, and said data processing apparatus, prepares a key file storing said encrypted content key data and encrypted  
15 usage control policy data indicating the handling of said content data, provides said content file provided from said data providing apparatus to said data distribution apparatus, and provides said prepared key file to said data processing apparatus,

20 said data distribution apparatus distributes said provided content file to said data processing apparatus, and

said data processing apparatus decrypts said content key data and said usage control policy data  
25 stored in said provided key file and determines the

handling of the content data stored in said distributed content file based on the related decrypted usage control policy data.

62. A data providing system comprising a data  
5 providing apparatus, a data distribution apparatus, a management apparatus, a database device, and a data processing apparatus, wherein

said data providing apparatus encrypts content data by using content key data, prepares a content file  
10 storing the related encrypted content data, and stores the related prepared content file and a key file provided from said management apparatus in said database device,

said management apparatus prepares the key file storing said encrypted content key data and encrypted  
15 usage control policy data indicating the handling of said content data, and provides the related prepared key file to said data providing apparatus,

said data distribution apparatus distributes said content file and key file obtained from said  
20 database device to said data processing apparatus, and

said data processing apparatus decrypts said content key data and said usage control policy data stored in said distributed key file and determines the handling of the content data stored in said distributed  
25 content file based on the related decrypted usage control

policy data.

63. A data providing system comprising a data  
providing apparatus, a data distribution apparatus, a  
management apparatus, a database device, and a data  
5 processing apparatus, wherein

said data providing apparatus encrypts content  
data by using content key data, prepares a content file  
storing the related encrypted content data, and stores  
the related prepared content file in said database  
10 device,

said management apparatus prepares the key file  
storing said encrypted content key data and encrypted  
usage control policy data indicating the handling of said  
content data and provides the related prepared key file  
15 to said data distribution apparatus,

said data distribution apparatus distributes  
said content file obtained from said database device and  
the key file provided from said data distribution  
apparatus to said data processing apparatus, and

20 said data processing apparatus decrypts said  
content key data and said usage control policy data  
stored in said distributed key file and determines the  
handling of the content data stored in said distributed  
content file based on the related decrypted usage control  
25 policy data.

64. A data providing system comprising a data providing apparatus, a data distribution apparatus, a management apparatus, a database device, and a data processing apparatus, wherein

5           said data providing apparatus encrypts content data by using content key data, prepares a content file storing the related encrypted content data, and stores the related prepared content file in said database device,

10           said management apparatus prepares the key file storing said encrypted content key data and encrypted usage control policy data indicating the handling of said content data and provides the related prepared key file to said data processing apparatus,

15           said data distribution apparatus distributes said content file obtained from said database device and the key file provided from said data distribution apparatus to said data processing apparatus, and

            said data processing apparatus decrypts said  
20 content key data and said usage control policy data stored in said provided key file and determines the handling of the content data stored in said distributed content file based on the related decrypted usage control policy data.

25           65. A data providing system comprising a plurality

of data providing apparatuses, a data distribution apparatus, a plurality of management apparatuses, a database device, and a data processing apparatus, wherein

5       said data providing apparatuses encrypt content data by using content key data, prepare content files storing the related encrypted content data, and store the related prepared content files and key files provided from corresponding management apparatuses in said database device,

10       said management apparatuses prepare key files storing said encrypted content key data and the encrypted usage control policy data indicating the handling of said content data for the content data provided by corresponding data providing apparatuses, and provide the  
15       related prepared key files to corresponding data providing apparatuses,

      said data distribution apparatus distributes said content files and key files obtained from said database device to said data processing apparatus, and

20       said data processing apparatus decrypts said content key data and said usage control policy data stored in said distributed key files and determines the handling of the content data stored in said distributed content files based on the related decrypted usage  
25       control policy data.

66. A data providing system comprising a plurality of data providing apparatuses, a data distribution apparatus, a plurality of management apparatuses, a database device, and a data processing apparatus, wherein

5           said data providing apparatuses encrypt content data by using content key data, prepare content files storing the related encrypted content data, and store the related prepared content files in said database device,

          said management apparatuses prepare key files

10          storing said encrypted content key data and the encrypted usage control policy data indicating the handling of said content data for the content data provided by corresponding data providing apparatuses, and provide the related prepared key files to said data distribution

15          apparatus,

          said data distribution apparatus distributes said content files obtained from said database device and the key files provided from said management apparatus to said data processing apparatus, and

20          said data processing apparatus decrypts said content key data and said usage control policy data stored in said distributed key files and determines the handling of the content data stored in said distributed content files based on the related decrypted usage

25          control policy data.



67. A data providing system comprising a plurality of data providing apparatuses, a data distribution apparatus, a plurality of management apparatuses, a database device, and a data processing apparatus, wherein

5           said data providing apparatuses encrypt content data by using content key data, prepare content files storing the related encrypted content data, and store the related prepared content files in said database device,

          said management apparatuses prepare key files  
10       storing said encrypted content key data and the encrypted usage control policy data indicating the handling of said content data for the content data provided by corresponding data providing apparatuses, and provide the related prepared key files to said data processing

15       apparatus,

          said data distribution apparatus distributes said content files obtained from said database device to said data processing apparatus, and

          said data processing apparatus decrypts said  
20       content key data and said usage control policy data stored in said distributed key files and determines the handling of the content data stored in said distributed content files based on the related decrypted usage control policy data.

25       68. A data providing system comprising a plurality

of data providing apparatuses, a data distribution apparatus, a plurality of management apparatuses, a database device, and a data processing apparatus, wherein

5       said data providing apparatuses provide master sources of content data to corresponding management apparatuses and store content files and key files received from the related management apparatuses in said database,

10       said management apparatuses encrypt said master sources received from corresponding data providing apparatuses by using content key data, prepare the content files storing the related encrypted content data, prepare key files storing said encrypted content key data and encrypted usage control policy data indicating the  
15       handling of said content data for the content data provided by corresponding data providing apparatuses, and send said prepared content files and said prepared key files to corresponding data providing apparatuses,

20       said data distribution apparatus distributes said content files and key files obtained from said database device to said data processing apparatus, and

      said data processing apparatus decrypts said content key data and said usage control policy data stored in said distributed key files and determines the  
25       handling of the content data stored in said distributed

content files based on the related decrypted usage control policy data.

69. A data providing system comprising a plurality of data providing apparatuses, a data distribution apparatus, a plurality of management apparatuses, a database device, and a data processing apparatus, wherein

10       said data providing apparatuses provide master sources of content data to corresponding management apparatuses, and store content files received from the related management apparatuses in said database,

15       said management apparatuses encrypt said master sources received from corresponding data providing apparatuses by using content key data, prepare the content files storing the related encrypted content data, send the related prepared content files to said data providing apparatuses, prepare key files storing said encrypted content key data and encrypted usage control policy data indicating the handling of said content data for the content data provided by corresponding data providing apparatuses, and send said prepared key files

20       to corresponding data distribution apparatus,

      said data distribution apparatus distributes said content files obtained from said database device and the key files provided from said management apparatuses

25       to said data processing apparatus, and

said data processing apparatus decrypts said content key data and said usage control policy data stored in said distributed key files and determines the handling of the content data stored in said distributed content files based on the related decrypted usage control policy data.

70. A data providing system comprising a plurality of data providing apparatuses, a data distribution apparatus, a plurality of management apparatuses, a database device, and a data processing apparatus, wherein

said data providing apparatuses provide master sources of content data to corresponding management apparatuses and store content files received from the related management apparatuses in said database,

said management apparatuses encrypt said master sources received from corresponding data providing apparatuses by using content key data, prepare the content files storing the related encrypted content data, send the related prepared content files to said data providing apparatuses, prepare key files storing said encrypted content key data and encrypted usage control policy data indicating the handling of said content data for the content data provided by corresponding data providing apparatuses, and send said prepared key files to said data processing apparatus,

said data distribution apparatus distributes  
said content files obtained from said database device and  
the key files provided from said management apparatuses  
to said data processing apparatus, and

5           said data processing apparatus decrypts said  
content key data and said usage control policy data  
stored in said provided key files and determines the  
handling of the content data stored in said distributed  
content files based on the related decrypted usage  
10 control policy data.

71. A data providing method for distributing  
content data from a data providing apparatus to a data  
processing apparatus and managing said data providing  
apparatus and said data processing apparatus by a  
15 management apparatus, wherein

said management apparatus prepares a key file  
storing encrypted content key data and encrypted usage  
control policy data indicating the handling of said  
content data,

20           said data providing apparatus provides said  
content data encrypted by using said content key data,  
and

said data processing apparatus decrypts said  
content key data and said usage control policy data  
25 stored in said key file and determines the handling of

said content data based on the related decrypted usage control policy data.

72. A data providing method for distributing content data from a data providing apparatus to a data processing apparatus and managing said data providing apparatus and said data processing apparatus by a management apparatus, comprising the steps of,

in said management apparatus, preparing a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of said content data,

distributing said prepared key file from said management apparatus to said data providing apparatus,

distributing a module storing a content file storing the content data encrypted by using said content key data and said key file distributed from said management apparatus from said data providing apparatus to said data processing apparatus, and

in said data processing apparatus, decrypting said content key data and said usage control policy data stored in said distributed module and determining the handling of said content data based on the related decrypted usage control policy data.

73. A data providing method for distributing content data from a data providing apparatus to a data

processing apparatus and managing said data providing  
apparatus and said data processing apparatus by a  
management apparatus, comprising the steps of,

in said management apparatus, preparing a key  
5 file storing encrypted content key data and encrypted  
usage control policy data indicating the handling of said  
content data,

in said data providing apparatus, distributing  
a module storing a content file containing the content  
10 data encrypted by using said content key data and the key  
file received from said management apparatus to said data  
processing apparatus, and

in said data processing apparatus, decrypting  
said content key data and said usage control policy data  
15 stored in said distributed module and determining the  
handling of said content data based on the related  
decrypted usage control policy data.

74. A data providing method for distributing  
content data from a data providing apparatus to a data  
20 processing apparatus and managing said data providing  
apparatus and said data processing apparatus by a  
management apparatus, comprising the steps of,

in said management apparatus, preparing a key  
file storing encrypted content key data and encrypted  
25 usage control policy data indicating the handling of said

content data,

distributing the related key file from said  
management apparatus to said data providing apparatus,

individually distributing a content file

5 storing the content data encrypted by using said content  
key data and said key file received from said management  
apparatus from said data providing apparatus to said data  
processing apparatus, and

10 in said data processing apparatus, decrypting  
said content key data and said usage control policy data  
stored in said distributed key file and determining the  
handling of the content data stored in said distributed  
content file based on the related decrypted usage control  
policy data.

15 75. A data providing method for distributing  
content data from a data providing apparatus to a data  
processing apparatus and managing said data providing  
apparatus and said data processing apparatus by a  
management apparatus, comprising the steps of,

20 in said management apparatus, preparing a key  
file storing encrypted content key data and encrypted  
usage control policy data indicating the handling of said  
content data,

distributing the related key file from said  
25 management apparatus to said data processing apparatus,



distributing a content file storing the content data encrypted by using said content key data from said data providing apparatus to said data processing apparatus, and

5           in said data processing apparatus, decrypting said content key data and said usage control policy data stored in said distributed key file and determining the handling of the content data stored in said distributed content file based on the related decrypted usage control  
10 policy data.

76. A data providing method for distributing content data from a data providing apparatus to a data processing apparatus and managing said data providing apparatus and said data processing apparatus by a  
15 management apparatus, comprising the steps of,

in said management apparatus, preparing a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of said content data,

20           in said data providing apparatus, distributing a module storing the content data encrypted by using said content key data and said key file received from said management apparatus to said data processing apparatus, and

25           in said data processing apparatus, decrypting

said content key data and said usage control policy data stored in said distributed module and determining the handling of said content data based on the related decrypted usage control policy data.

5           77. A data providing method for distributing content data from a data providing apparatus to a data processing apparatus and managing said data providing apparatus and said data processing apparatus by a management apparatus, comprising the steps of,

10                 in said management apparatus, preparing a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of said content data,

                  in said data providing apparatus, individually  
15     distributing the content data encrypted by using said content key data and said key file received from said management apparatus to said data processing apparatus, and

                  in said data processing apparatus, decrypting  
20     said content key data and said usage control policy data stored in said distributed key file and determining the handling of said distributed content data based on the related decrypted usage control policy data.

                  78. A data providing method for distributing  
25     content data from a data providing apparatus to a data

processing apparatus and managing said data providing  
apparatus and said data processing apparatus by a  
management apparatus, comprising the steps of,

in said management apparatus, preparing a key  
5 file storing encrypted content key data and encrypted  
usage control policy data indicating the handling of said  
content data,

distributing the related prepared key file to  
said data processing apparatus,

10 in said data providing apparatus, distributing  
the content data encrypted by using said content key data  
to said data processing apparatus, and

in said data processing apparatus, decrypting  
said content key data and said usage control policy data  
15 stored in said distributed key file and determining the  
handling of said distributed content data based on the  
related decrypted usage control policy data.

79. A data providing method for distributing  
content data from a data providing apparatus to a data  
20 processing apparatus and managing said data providing  
apparatus and said data processing apparatus by a  
management apparatus, comprising the steps of,

in said management apparatus, preparing  
encrypted content key data and encrypted usage control  
25 policy data indicating the handling of said content data,

in said data providing apparatus, individually  
distributing the content data encrypted by using said  
content key data and said encrypted content key data and  
said encrypted usage control policy data received from  
5 said management apparatus to said data processing  
apparatus, and

in said data processing apparatus, decrypting  
said distributed content key data and said usage control  
policy data and determining the handling of the content  
10 data stored in said distributed content file based on the  
related decrypted usage control policy data.

80. A data providing method for distributing  
content data from a data providing apparatus to a data  
processing apparatus and managing said data providing  
15 apparatus and said data processing apparatus by a  
management apparatus, comprising the steps of,

in said management apparatus, preparing  
encrypted content key data and encrypted usage control  
policy data indicating the handling of said content data  
20 and distributing the same to said data processing  
apparatus,

in said data providing apparatus, distributing  
the content data encrypted by using said content key data  
to said data processing apparatus, and

25 in said data processing apparatus, decrypting

said distributed content key data and said usage control policy data and determining the handling of said distributed content data based on the related decrypted usage control policy data.

5           81. A data providing method using a data providing apparatus, a data distribution apparatus, a data processing apparatus, and a management apparatus, comprising the steps of,

10                 in said management apparatus, preparing a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of said content data,

15                 providing said content data encrypted by using said content key data from said data providing apparatus to said data distribution apparatus,

                  in said data distribution apparatus, distributing said provided content data to said data processing apparatus, and

20                 in said data processing apparatus, decrypting said content key data and said usage control policy data stored in said key file and determining the handling of said distributed content data based on the related decrypted usage control policy data.

25           82. A data providing method for providing content data from a data providing apparatus to a data

distribution apparatus, distributing the content data  
from said data distribution apparatus to a data  
processing apparatus, and managing said data providing  
apparatus, said data distribution apparatus, and said  
5 data processing apparatus by a management apparatus,  
comprising the steps of,

in said management apparatus, preparing a key  
file storing encrypted content key data and encrypted  
usage control policy data indicating the handling of said  
10 content data,

distributing the related prepared key file from  
said management apparatus to said data providing  
apparatus,

providing a first module storing a content file  
15 storing the content data encrypted by using said content  
key data and said key file received from said management  
apparatus from said data providing apparatus to said data  
distribution apparatus, and

distributing a second module storing said  
20 provided content file and said key file from said data  
distribution apparatus to said data processing apparatus,  
and

in said data processing apparatus, decrypting  
said content key data and said usage control policy data  
25 stored in said distributed second module and determining

the handling of said content data stored in said distributed second module based on the related decrypted usage control policy data.

83. A data providing method for providing content data from a data providing apparatus to a data distribution apparatus, distributing the content data from said data distribution apparatus to a data processing apparatus, and managing said data providing apparatus, said data distribution apparatus, and said data processing apparatus by a management apparatus, comprising the steps of,

in said management apparatus, preparing a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of said content data,

in said data providing apparatus, providing a first module storing a content file containing the content data encrypted by using said content key data and a key file received from said management apparatus to said data distribution apparatus,

in said data distribution apparatus, distributing a second module storing said provided content file to said data processing apparatus, and

in said data processing apparatus, decrypting said content key data and said usage control policy data

stored in said distributed second module and determining the handling of said content data stored in said distributed second module based on the related decrypted usage control policy data.

- 5           84. A data providing method for providing content data from a data providing apparatus to a data distribution apparatus, distributing the content data from said data distribution apparatus to a data processing apparatus, and managing said data providing
- 10 apparatus, said data distribution apparatus, and said data processing apparatus by a management apparatus, comprising the steps of,
- in said management apparatus, preparing a key file storing encrypted content key data and encrypted
- 15 usage control policy data indicating the handling of said content data,
- distributing said prepared key file from said management apparatus to said data providing apparatus,
- individually distributing a content file
- 20 storing the content data encrypted by using said content key data and said key file received from said management apparatus from said data providing apparatus to said data distribution apparatus,
- individually distributing said distributed
- 25 content file and said key file from said data



distribution apparatus to said data distribution  
apparatus, and

in said data processing apparatus, decrypting  
said content key data and said usage control policy data  
5 stored in said distributed key file and determining the  
handling of the content data stored in said distributed  
content file based on the related decrypted usage control  
policy data.

85. A data providing method for distributing  
10 content data from a data providing apparatus to a data  
processing apparatus and managing said data providing  
apparatus and said data processing apparatus by a  
management apparatus, comprising the steps of,

in said management apparatus, preparing a key  
15 file storing encrypted content key data and encrypted  
usage control policy data indicating the handling of said  
content data,

distributing the related prepared key file from  
said management apparatus to said data processing  
20 apparatus,

providing a content file storing the content  
data encrypted by using said content key data from said  
data providing apparatus to said data distribution  
apparatus, and

25 distributing said provided content file from

said data distribution apparatus to said data processing apparatus, and

in said data processing apparatus, decrypting said content key data and said usage control policy data stored in said distributed key file and determining the  
5 handling of the content data stored in said distributed content file based on the related decrypted usage control policy data.

86. A data providing method for providing content  
10 data from a data providing apparatus to a data distribution apparatus, distributing the content data from said data distribution apparatus to a data processing apparatus, and managing said data providing apparatus, said data distribution apparatus, and said  
15 data processing apparatus by a management apparatus, comprising the steps of,

in said management apparatus, preparing a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of said  
20 content data,

in said data providing apparatus, providing a first module storing the content data encrypted by using said content key data and said key file received from said management apparatus to said data distribution  
25 apparatus,

in said data distribution apparatus,  
distributing a second module storing said provided  
content data and said key file to said data processing  
apparatus, and

5 in said data processing apparatus, decrypting  
said content key data and said usage control policy data  
stored in said distributed second module and determining  
the handling of said content data stored in said  
distributed second module based on the related decrypted  
10 usage control policy data.

87. A data providing method for providing content  
data from a data providing apparatus to a data  
distribution apparatus, distributing the content data  
from said data distribution apparatus to a data  
15 processing apparatus, and managing said data providing  
apparatus, said data distribution apparatus, and said  
data processing apparatus by a management apparatus,  
comprising the steps of,

in said management apparatus, preparing a key  
20 file storing encrypted content key data and encrypted  
usage control policy data indicating the handling of said  
content data,

in said data providing apparatus, individually  
distributing the content data encrypted by using said  
25 content key data and said key file received from said

management apparatus to said data distribution apparatus,  
in said data distribution apparatus,  
individually distributing said distributed content data  
and said key file to said data distribution apparatus,  
5 and

in said data processing apparatus, decrypting  
said content key data and said usage control policy data  
stored in said distributed key file and determining the  
handling of said distributed content data based on the  
10 related decrypted usage control policy data.

88. A data providing method for distributing  
content data from a data providing apparatus to a data  
processing apparatus and managing said data providing  
apparatus and said data processing apparatus by a  
15 management apparatus, comprising the steps of,

in said management apparatus, preparing a key  
file storing encrypted content key data and encrypted  
usage control policy data indicating the handling of said  
content data and distributing the related prepared key  
20 file to said data processing apparatus,

in said data providing apparatus, providing the  
content data encrypted by using said content key data to  
said data distribution apparatus,

in said data distribution apparatus,  
25 distributing said provided content data to said data

processing apparatus, and

in said data processing apparatus, decrypting  
said content key data and said usage control policy data  
stored in said distributed key file and determining the  
5 handling of said distributed content data based on the  
related decrypted usage control policy data.

89. A data providing method for providing content  
data from a data providing apparatus to a data  
distribution apparatus, distributing the content data  
10 from said data distribution apparatus to a data  
processing apparatus, and managing said data providing  
apparatus, said data distribution apparatus, and said  
data processing apparatus by a management apparatus,  
comprising the steps of,

15 in said management apparatus, providing  
encrypted content key data and encrypted usage control  
policy data indicating the handling of said content data  
to said data providing apparatus,

in said data providing apparatus, individually  
20 distributing the content data encrypted by using said  
content key data and said encrypted content key data and  
said encrypted usage control policy data which are  
received from said management apparatus to said data  
distribution apparatus,

25 in said data distribution apparatus,

individually distributing said distributed content data,  
said encrypted content key data, and said encrypted usage  
control policy data to said data distribution apparatus,  
and

5                   in said data processing apparatus, decrypting  
said distributed content key data and said usage control  
policy data and determining the handling of said  
distributed content data based on the related decrypted  
usage control policy data.

10           90. A data providing method for providing content  
data from a data providing apparatus to a data  
distribution apparatus, distributing the content data  
from said data distribution apparatus to a data  
processing apparatus, and managing said data providing  
15   apparatus, said data distribution apparatus, and said  
data processing apparatus by a management apparatus,  
comprising the steps of,

                  in said management apparatus, distributing  
encrypted content key data and encrypted usage control  
20   policy data indicating the handling of said content data  
to said data processing apparatus,

                  in said data providing apparatus, distributing  
the content data encrypted by using said content key data  
to said data distribution apparatus,

25                   in said data distribution apparatus,

distributing said provided content data to said data processing apparatus, and

in said data processing apparatus, decrypting said distributed content key data and said usage control policy data and determining the handling of said distributed content data based on the related decrypted usage control policy data.

91. A data providing method using a data providing apparatus, a data distribution apparatus, a management apparatus, and a data processing apparatus, wherein said data providing apparatus provides master source data of content to said management apparatus, said management apparatus manages said data providing apparatus, said data distribution apparatus, and said data processing apparatus, encrypts said provided master source data by using content key data to prepare content data, prepares a content file storing the related content data, prepares a key file storing said encrypted content key data and encrypted usage control policy data indicating the handling of said content data, and provides said content file and said key file to said data distribution apparatus,

said data distribution apparatus distributes said provided content file and said key file to said data processing apparatus, and

said data processing apparatus decrypts said content key data and said usage control policy data stored in said distributed key file and determines the handling of the content data stored in said distributed content file based on the related decrypted usage control policy data.

92. A data providing method using a data providing apparatus, a data distribution apparatus, a management apparatus, and a data processing apparatus, wherein

10           said data providing apparatus provides master source data of content to said management apparatus,

              said management apparatus manages said data providing apparatus, said data distribution apparatus, and said data processing apparatus, encrypts said

15   provided master source data by using content key data to prepare content data, prepares a content file storing the related content data, prepares a key file storing said encrypted content key data and encrypted usage control policy data indicating the handling of said content data,

20   and provides said content file to said data distribution apparatus and provides said key file to said data processing apparatus,

              said data distribution apparatus distributes said provided content file to said data processing

25   apparatus, and



said data processing apparatus decrypts said content key data and said usage control policy data stored in said provided key file and determines the handling of the content data stored in said distributed content file based on the related decrypted usage control policy data.

93. A data providing method using a data providing apparatus, a data distribution apparatus, a management apparatus, and a data processing apparatus, wherein said data providing apparatus provides a content file storing encrypted content data using content key data to said management apparatus,

said management apparatus manages said data providing apparatus, said data distribution apparatus, and said data processing apparatus, prepares a key file storing said encrypted content key data and encrypted usage control policy data indicating the handling of said content data, provides said content file provided from said data providing apparatus and said prepared key file to said data distribution apparatus,

said data distribution apparatus distributes said provided content file and said key file to said data processing apparatus, and

said data processing apparatus decrypts said content key data and said usage control policy data

stored in said distributed key file and determines the handling of the content data stored in said distributed content file based on the related decrypted usage control policy data.

5           94. A data providing method using a data providing apparatus, a data distribution apparatus, a management apparatus, and a data processing apparatus, wherein

                  said data providing apparatus provides a content file storing encrypted content data using content  
10 key data to said management apparatus,

                  said management apparatus manages said data providing apparatus, said data distribution apparatus, and said data processing apparatus, prepares a key file storing said encrypted content key data and encrypted  
15 usage control policy data indicating the handling of said content data, provides said content file provided from said data providing apparatus to said data distribution apparatus, and provides said prepared key file to said data processing apparatus,

20           said data distribution apparatus distributes said provided content file to said data processing apparatus, and

                  said data processing apparatus decrypts said content key data and said usage control policy data  
25 stored in said provided key file and determines the

handling of the content data stored in said distributed content file based on the related decrypted usage control policy data.

95. A data providing method using a data providing apparatus, a data distribution apparatus, a management apparatus, a database device, and a data processing apparatus, wherein

said data providing apparatus encrypts content data by using content key data, prepares a content file storing the related encrypted content data, and stores the related prepared content file and a key file provided from said management apparatus in said database device,

said management apparatus prepares a key file storing said encrypted content key data and encrypted usage control policy data indicating the handling of said content data and provides the related prepared key file to said data providing apparatus,

said data distribution apparatus distributes said content file and key file obtained from said database device to said data processing apparatus, and

said data processing apparatus decrypts said content key data and said usage control policy data stored in said distributed key file and determines the handling of the content data stored in said distributed content file based on the related decrypted usage control

policy data.

96. A data providing method using a data providing  
apparatus, a data distribution apparatus, a management  
apparatus, a database device, and a data processing  
5 apparatus, wherein

said data providing apparatus encrypts content  
data by using content key data, prepares a content file  
storing the related encrypted content data, and stores  
the related prepared content file in said database  
10 device,

said management apparatus prepares a key file  
storing said encrypted content key data and encrypted  
usage control policy data indicating the handling of said  
content data and provides the related prepared key file  
15 to said data distribution apparatus,

said data distribution apparatus distributes  
said content file obtained from said database device and  
the key file provided from said data distribution  
apparatus to said data processing apparatus, and

20 said data processing apparatus decrypts said  
content key data and said usage control policy data  
stored in said distributed key file and determines the  
handling of the content data stored in said distributed  
content file based on the related decrypted usage control  
25 policy data.

97. A data providing method using a data providing apparatus, a data distribution apparatus, a management apparatus, a database device, and a data processing apparatus, wherein

5           said data providing apparatus encrypts content data by using content key data, prepares a content file storing the related encrypted content data, and stores the related prepared content file in said database device,

10           said management apparatus prepares a key file storing said encrypted content key data and encrypted usage control policy data indicating the handling of said content data and provides the related prepared key file to said data processing apparatus,

15           said data distribution apparatus distributes said content file obtained from said database device and the key file provided from said data distribution apparatus to said data processing apparatus, and

            said data processing apparatus decrypts said  
20 content key data and said usage control policy data stored in said provided key file and determines the handling of the content data stored in said distributed content file based on the related decrypted usage control policy data.

25           98. A data providing method using a plurality of

data providing apparatuses, a data distribution apparatus, a plurality of management apparatuses, a database device, and a data processing apparatus, wherein

5       said data providing apparatuses encrypt content data by using content key data, prepare content files storing the related encrypted content data, and store the related prepared content files and key files provided from corresponding management apparatuses in said database device,

10               said management apparatuses prepare the key files storing said encrypted content key data and encrypted usage control policy data indicating the handling of said content data for the content data provided by corresponding data providing apparatuses and  
15       provide the related prepared key files to corresponding data providing apparatuses,

              said data distribution apparatus distributes said content files and key files obtained from said database device to said data processing apparatus, and  
20               said data processing apparatus decrypts said content key data and said usage control policy data stored in said distributed key files and determines the handling of the content data stored in said distributed content files based on the related decrypted usage  
25       control policy data.

99. A data providing method using a plurality of data providing apparatuses, a data distribution apparatus, a plurality of management apparatuses, a database device, and a data processing apparatus, wherein

5           said data providing apparatuses encrypt content data by using content key data, prepare content files storing the related encrypted content data, and store the related prepared content files in said database device,

                  said management apparatuses prepare the key  
10   files storing said encrypted content key data and encrypted usage control policy data indicating the handling of said content data for the content data provided by corresponding data providing apparatuses and provide the related prepared key files to said data  
15   distribution apparatus,

                  said data distribution apparatus distributes said content files obtained from said database device and the key files provided from said management apparatuses to said data processing apparatus, and

20           said data processing apparatus decrypts said content key data and said usage control policy data stored in said distributed key files and determines the handling of the content data stored in said distributed content files based on the related decrypted usage  
25   control policy data.

100. A data providing method using a plurality of data providing apparatuses, a data distribution apparatus, a plurality of management apparatuses, a database device, and a data processing apparatus, wherein

5           said data providing apparatuses encrypt content data by using content key data, prepare content files storing the related encrypted content data, and store the related prepared content files in said database device,

          said management apparatuses prepare the key  
10   files storing said encrypted content key data and encrypted usage control policy data indicating the handling of said content data for the content data provided by corresponding data providing apparatuses and provide the related prepared key files to said data  
15   processing apparatus,

          said data distribution apparatus distributes said content files obtained from said database device to said data processing apparatus, and

          said data processing apparatus decrypts said  
20   content key data and said usage control policy data stored in said provided key files and determines the handling of the content data stored in said distributed content files based on the related decrypted usage control policy data.

25           101. A data providing method using a plurality of



data providing apparatuses, a data distribution apparatus, a plurality of management apparatuses, a database device, and a data processing apparatus, wherein

5       said data providing apparatuses provide master sources of content data to corresponding management apparatuses and store content files and key files received from the related management apparatuses in said database,

10       said management apparatuses encrypt said master sources received from corresponding data providing apparatuses by using content key data, prepare content files storing the related encrypted content data, prepare key files storing said encrypted content key data and encrypted usage control policy data indicating the  
15       handling of said content data for the content data provided by corresponding data providing apparatuses, and send said prepared content files and said prepared key files to corresponding data providing apparatuses,

20       said data distribution apparatus distributes said content files and key files obtained from said database device to said data processing apparatus, and

      said data processing apparatus decrypts said content key data and said usage control policy data stored in said distributed key files and determines the  
25       handling of the content data stored in said distributed

content files based on the related decrypted usage control policy data.

102. A data providing method using a plurality of data providing apparatuses, a data distribution apparatus, a plurality of management apparatuses, a database device, and a data processing apparatus, wherein

5       said data providing apparatuses provide master sources of content data to corresponding management apparatuses and store content files received from the related management apparatuses in said database,

10       said management apparatuses encrypt said master sources received from corresponding data providing apparatuses by using content key data, prepare content files storing the related encrypted content data, send

15       the related prepared content files to said data providing apparatuses, prepare key files storing said encrypted content key data and encrypted usage control policy data indicating the handling of said content data for the content data provided by corresponding data providing

20       apparatuses, and send the related prepared key files to corresponding data distribution apparatus,

      said data distribution apparatus distributes said content files obtained from said database device and key files provided from said management apparatuses to

25       said data processing apparatus, and

said data processing apparatus decrypts said content key data and said usage control policy data stored in said distributed key files and determines the handling of the content data stored in said distributed content files based on the related decrypted usage control policy data.

103. A data providing method using a plurality of data providing apparatuses, a data distribution apparatus, a plurality of management apparatuses, a database device, and a data processing apparatus, wherein

said data providing apparatuses provide master sources of content data to corresponding management apparatuses and store content files received from the related management apparatuses in said database,

15 said management apparatuses encrypt said master sources received from corresponding data providing apparatuses by using content key data, prepare content files storing the related encrypted content data, send the related prepared content files to said data providing apparatuses, prepare key files storing said encrypted content key data and encrypted usage control policy data indicating the handling of said content data for the content data provided by corresponding data providing apparatuses, and provide the related prepared key files  
20 to said data processing apparatus,

said data distribution apparatus distributes  
said content files obtained from said database device to  
said data processing apparatus, and

said data processing apparatus decrypts said  
5 content key data and said usage control policy data  
stored in said provided key files and determines the  
handling of the content data stored in said distributed  
content files based on the related decrypted usage  
control policy data.

10 104. A data providing system for distributing  
content data from a data providing apparatus to a data  
processing apparatus, wherein

said data providing apparatus distributes a  
module storing the content data encrypted by using  
15 content key data, said encrypted content key data, and  
encrypted usage control policy data indicating the  
handling of said content data to said data processing  
apparatus by using a predetermined communication protocol  
in a format not depending upon the related communication  
20 protocol or by recording the same on a storage medium,  
and

said data processing apparatus decrypts said  
content key data and said usage control policy data  
stored in said distributed module and determines the  
25 handling of said content data based on the related

decrypted usage control policy data.

105. A data providing system as set forth in claim  
104, wherein said data providing apparatus distributes  
said module further storing signature data for verifying  
5 a legitimacy of a producer and a transmitter of at least  
one data among said content data, said content key data,  
and said usage control policy data to said data  
processing apparatus.

106. A data providing system as set forth in claim  
10 104, wherein  
said data providing apparatus distributes said  
module further storing at least one data between data for  
verifying if the related data is not tampered with and  
signature data for verifying if the related data was  
15 normally certified by a predetermined manager for at  
least one data among said content data, said content key  
data, and said usage control policy data to said data  
processing apparatus.

107. A data providing system as set forth in claim  
20 104, wherein  
said data processing apparatus determines a  
purchase form of said content data based on said usage  
control policy data, and

where said content data is transferred to  
25 another data processing apparatus, the signature data

indicating the legitimacy of the purchaser of the related content data and the signature data indicating the legitimacy of the transmitter of the related content data are made different.

5           108. A data providing system as set forth in claim 104, wherein said data providing apparatus produces signature data using secret key data of said data providing apparatus and a hash function.

10           109. A data providing system for distributing content data from a data providing apparatus to a data processing apparatus and managing said data providing apparatus and said data processing apparatus by a management apparatus, wherein

15               said management apparatus prepares a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of said content data,

20               said data providing apparatus distributes a module storing a content file storing the content data encrypted by using said content key data and said key file received from said management apparatus to said data processing apparatus by using a predetermined communication protocol in a format not depending upon the related communication protocol or by recording the same  
25           on a storage medium, and

said data processing apparatus decrypts said content key data and said usage control policy data stored in said distributed module and determines the handling of said content data based on the related  
5 decrypted usage control policy data.

110. A data providing system as set forth in claim 109, wherein said management apparatus produces signature data for verifying the legitimacy of the producer of said key file and prepares said key file further storing the  
10 related signature data.

111. A data providing system as set forth in claim 109, wherein

said data providing apparatus produces said content key data and said usage control policy data and  
15 transmits the same to said management apparatus, and

said management apparatus prepares said key file based on said received content key data and usage control policy data and registers the related prepared key file.

20 112. A data providing system as set forth in claim 110, wherein said data providing apparatus produces signature data for verifying at least one of the legitimacy of a producer and transmitter of said content file and a distributor of said key file and distributes  
25 said module further storing said signature data to said

data processing apparatus.

113. A data providing system as set forth in claim 112, wherein said data processing apparatus verifies the signature data stored in said module to confirm at least one of the legitimacy of a producer and distributor of said content file and a producer and distributor of said key file.

114. A data providing system as set forth in claim 109, wherein said data providing apparatus further stores in said content file expansion use software for expanding the content data when the content data is compressed.

115. A data providing system as set forth in claim 109, wherein said data providing apparatus further stores in said content file an electronic watermark information module including information used for detecting said electronic watermark information when electronic watermark information is buried in said content file.

116. A data providing system as set forth in claim 109, wherein said data providing apparatus stores metadata relating to the explanation of the content of the content data in said content file or distributes it separately from the content file to said data processing apparatus.

117. A data providing system as set forth in claim 109, wherein



said management apparatus produces said key file storing said content file data and said usage control policy data encrypted using said distribution use key data.

5           118. A data providing system as set forth in claim 117, wherein said management apparatus and said data processing apparatus comprise a plurality of distribution use key data of defined periods of validity and use distribution use key data of corresponding periods.

10           119. A data providing system as set forth in claim 109, wherein said management apparatus produces said key file further storing data describing the grammar of said usage policy control data.

15           120. A data providing system as set forth in claim 109, wherein  
              said management apparatus distributes data showing information for reading the content file and the key file, that is, a file reader, to said data processing apparatus and

20           said data processing apparatus reads said content file and said key file based on the file reader.

              121. A data providing system as set forth in claim 109, wherein

              said data providing apparatus distributes data  
25           showing information for reading the content file and the

key file, that is, a file reader, to said data processing apparatus and

said data processing apparatus reads said content file and said key file based on the file reader.

5        122. A data providing system as set forth in claim 113, wherein

said data providing apparatus produces said signature data using its own secret key data and

10        said data processing apparatus verifies the legitimacy of said signature data using public key data corresponding to said secret key data.

123. A data providing system as set forth in claim 122, wherein

15        said data providing apparatus distributes said module further storing public key certificate data certifying the legitimacy of said public key data to said data processing apparatus and

20        said data processing apparatus verifies said signature data using the public key data stored in said distributed public key certificate data.

124. A data providing system as set forth in claim 122, wherein

25        said management apparatus distributes public key certificate data certifying the legitimacy of said public key data to said data processing apparatus and

said data processing apparatus verifies said signature data using the public key data stored in said distributed public key certificate data.

125. A data providing system as set forth in claim  
5 122, wherein said data providing apparatus performs mutual certification with said data processing apparatus, encrypts said module using session key data obtained by said mutual certification, and sends the encrypted module to said data processing apparatus.

10 126. A data providing system as set forth in claim 122, wherein said data providing apparatus produces a storage medium recording said module.

127. A data providing system as set forth in claim  
15 122, wherein said data processing apparatus determines at least one of a purchase form and a usage form of said content data based on said usage control policy data.

128. A data providing system as set forth in claim  
20 122, wherein said data processing apparatus outputs said encrypted content key data and said encrypted content data to a decryption device.

129. A data providing system as set forth in claim  
129, wherein

said data processing apparatus determines at  
least one of the purchase form and the usage form of the  
25 distributed content data based on the usage control

policy data and sends log data showing the log of at least one of the purchase form and usage form decided to said management apparatus, and

said management apparatus performs profit  
5 distribution processing for distributing the profit obtained along with the purchase and usage of the content data in the data processing apparatus to the interested parties of the data providing apparatus based on the received log data.

10 130. A data providing system as set forth in claim 129, wherein said management apparatus performs said profit distribution processing in units of content data.

131. A data providing system as set forth in claim 129, wherein

15 said data providing apparatus distributes a module storing a plurality of said content files and a plurality of key files corresponding to the plurality of content files to said data processing apparatus and

said content files include directory structure  
20 data showing the relationship among the plurality of content files and the relationship with said key files.

132. A data providing system as set forth in claim 109, wherein said data providing apparatus further comprises a memory circuit for storing said module.

25 133. A data providing system as set forth in claim

132, wherein said data providing apparatus manages said module based on a content identifier uniquely allocated to said content data.

134. A data providing system as set forth in claim 5 133, wherein said management apparatus prepares said key file further storing said content identifier.

135. A data providing system as set forth in claim 133, wherein said content identifier is determined uniquely in said content data stored by said data 10 providing apparatus in said memory circuit.

136. A data providing system as set forth in claim 133, wherein said content identifier is determined uniquely globally.

137. A data providing system as set forth in claim 15 133, wherein said data providing apparatus produces said content identifier.

138. A data providing system as set forth in claim 133, wherein said data providing apparatus further comprises a memory circuit for storing said module.

20 139. A data providing system as set forth in claim 133, wherein said data processing circuit comprises a module giving resistance to outside monitoring and tampering of the processing content, predetermined data stored in an internal memory, and data being processed.

25 140. A data providing apparatus which is managed by

a management apparatus and distributes content data to a data processing apparatus,

receiving a key file storing encrypted content key data and encrypted usage control policy data

5 indicating the handling of said content data from said management apparatus and

distributing a module storing a content file storing the content data encrypted by using said content key data and said key file received from said management apparatus to said data processing apparatus.

141. A data processing apparatus managed by a management apparatus and utilizing content data,

receiving a module containing a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of said content data and a content file storing the content data encrypted by using said content key data,

determining at least one between a purchase form and an usage form of said content data based on said usage control policy data, and

transmitting a log data indicating the log of the determined at least one of the related purchase form and usage form to said management apparatus.

142. A data providing system for distributing content data from a data providing apparatus to a data

processing apparatus and managing said data providing  
apparatus and said data processing apparatus by a  
management apparatus, wherein

5       said management apparatus prepares a key file  
storing encrypted content key data and encrypted usage  
control policy data indicating the handling of said  
content data,

      said data providing apparatus distributes a  
module storing a content file containing the content data  
10   encrypted by using said content key data and the key file  
received from said management apparatus to said data  
processing apparatus by using a predetermined  
communication protocol in a format not depending upon the  
related communication protocol or recording the same on a  
15   storage medium, and

      said data processing apparatus decrypts said  
content key data and said usage control policy data  
stored in said distributed module and determines the  
handling of said content data based on the related  
20   decrypted usage control policy data.

143. A data providing system for distributing  
content data from a data providing apparatus to a data  
processing apparatus and managing said data providing  
apparatus and said data processing apparatus by a  
25   management apparatus, wherein

said management apparatus prepares a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of said content data,

5           said data providing apparatus individually distributes a content file storing the content data encrypted by using said content key data and said key file received from said management apparatus to said data processing apparatus by using a predetermined  
10 communication protocol but in a format not depending upon the related communication protocol or by recording the same on a storage medium, and

          said data processing apparatus decrypts said content key data and said usage control policy data  
15 stored in said distributed key file and determines the handling of the content data stored in said distributed content file based on the related decrypted usage control policy data.

144. A data providing system as set forth in claim  
20 143, wherein

          said data providing apparatus individually distributes a plurality of said content files and a plurality of key files corresponding to said plurality of content files to said data processing apparatus, and  
25           said content files and said key files include



hyper link information showing the mutual correspondence.

145. A data providing system for distributing  
content data from a data providing apparatus to a data  
processing apparatus and managing said data providing  
5 apparatus and said data processing apparatus by a  
management apparatus, wherein

said management apparatus prepares a key file  
storing encrypted content key data and encrypted usage  
control policy data indicating the handling of said  
10 content data and distributes the related prepared key  
file to said data processing apparatus,

said data providing apparatus distributes a  
content file storing the content data encrypted by using  
said content key data to said data processing apparatus  
15 by using a predetermined communication protocol but in a  
format not depending upon the related communication  
protocol or recording the same on a storage medium, and

said data processing apparatus decrypts said  
content key data and said usage control policy data  
20 stored in said distributed key file and determines the  
handling of the content data stored in said distributed  
content file based on the related decrypted usage control  
policy data.

146. A data providing system as set forth in claim  
25 145, wherein

said data providing apparatus distributes a plurality of said content files to said data processing apparatus,

said management apparatus distributes the  
5 plurality of key files corresponding to the plurality of content files to said data processing apparatus, and

said content files and said key files include hyper link information showing the mutual correspondence.

147. A data providing system for distributing  
10 content data from a data providing apparatus to a data processing apparatus and managing said data providing apparatus and said data processing apparatus by a management apparatus, wherein

said management apparatus prepares a key file  
15 storing encrypted content key data and encrypted usage control policy data indicating the handling of said content data,

said data providing apparatus distributes a module storing the content data encrypted by using said  
20 content key data and said key file received from said management apparatus to said data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and

25 said data processing apparatus decrypts said

content key data and said usage control policy data stored in said distributed module and determines the handling of said content data based on the related decrypted usage control policy data.

5           148. A data providing system for distributing content data from a data providing apparatus to a data processing apparatus and managing said data providing apparatus and said data processing apparatus by a management apparatus, wherein

10                   said management apparatus prepares a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of said content data,

                  said data providing apparatus individually  
15 distributes the content data encrypted by using said content key data and said key file received from said management apparatus to said data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication  
20 protocol or recording the same on a storage medium, and

                  said data processing apparatus decrypts said content key data and said usage control policy data stored in said distributed key file and determines the handling of said distributed content data based on the  
25 related decrypted usage control policy data.

149. A data providing system for distributing content data from a data providing apparatus to a data processing apparatus and managing said data providing apparatus and said data processing apparatus by a management apparatus, wherein

5       said management apparatus prepares a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of said content data and distributes the related prepared key  
10   file to said data processing apparatus,

      said data providing apparatus distributes the content data encrypted by using said content key data to said data processing apparatus by using a predetermined communication protocol but in a format not depending upon  
15   the related communication protocol or recording the same on a storage medium, and

      said data processing apparatus decrypts said content key data and said usage control policy data stored in said distributed key file and determines the  
20   handling of said distributed content data based on the related decrypted usage control policy data.

150. A data providing system for distributing content data from a data providing apparatus to a data processing apparatus and managing said data providing apparatus and said data processing apparatus by a  
25   apparatus and said data processing apparatus by a

management apparatus, wherein

said management apparatus prepares encrypted content key data and encrypted usage control policy data indicating the handling of said content data,

5           said data providing apparatus individually distributes the content data encrypted by using said content key data and said encrypted content key data and said encrypted usage control policy data received from said management apparatus to said data processing  
10   apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and

          said data processing apparatus decrypts said  
15   distributed content key data and said usage control policy data and determines the handling of the content data stored in said distributed content file based on the related decrypted usage control policy data.

151. A data providing system for distributing  
20   content data from a data providing apparatus to a data processing apparatus and managing said data providing apparatus and said data processing apparatus by a management apparatus, wherein

          said management apparatus prepares encrypted  
25   content key data and encrypted usage control policy data

indicating the handling of said content data and  
distributes the same to said data processing apparatus,  
said data providing apparatus distributes the  
content data encrypted by using said content key data to  
5 said data processing apparatus by using a predetermined  
communication protocol but in a format not depending upon  
the related communication protocol or recording the same  
on a storage medium, and

10 said data processing apparatus decrypts said  
distributed content key data and said usage control  
policy data and determines the handling of said  
distributed content data based on the related decrypted  
usage control policy data.

15 152. A data providing system comprising a data  
providing apparatus, a data distribution apparatus, and a  
data processing apparatus, wherein

20 said data providing apparatus provides a first  
module storing content data encrypted by using content  
key data, said encrypted content key data, and encrypted  
usage control policy data indicating the handling of said  
content data to said data distribution apparatus,

said data distribution apparatus distributes a  
second module storing said encrypted content data,  
content key data, and the usage control policy data  
25 stored in said provided first module to said data

processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or by recording the same on a storage medium, and

5           said data processing apparatus decrypts said content key data and said usage control policy data stored in said distributed second module and determines the handling of said content data based on the related decrypted usage control policy data.

10           153. A data providing system as set forth in claim 152, wherein said data distribution apparatus prepares a second module including said provided first module and distributes the prepared second module to said data processing apparatus.

15           154. A data providing system as set forth in claim 152, wherein said data distribution apparatus distributes said second module further storing price data showing the price of the content data to said data processing apparatus.

20           155. A data providing system as set forth in claim 154, wherein said data distribution apparatus determines the price data based on a wholesale price determined for said content data by said data providing apparatus.

            156. A data providing system as set forth in claim  
25   152, wherein said data providing apparatus provides a

first module further storing signature data for verifying the legitimacy of a producer and transmitter of at least one data of the content data, content key data, and usage control policy data to said data distribution apparatus.

5           157. A data providing system as set forth in claim 156, wherein said data providing apparatus provides a first module further storing at least one data among data for verifying if the data has been tampered with for at least one data of the content data, content key data, and  
10           usage control policy data and signature data for verifying if the data has been certified as legitimate by a predetermined manager to said data distribution device.

          158. A data providing system as set forth in claim 156, wherein said data distribution apparatus provides  
15           said second module further storing signature data for verifying the legitimacy of a producer and transmitter of at least one data among the content data, content key data, and usage control policy data to said data processing apparatus.

20           159. A data providing system as set forth in claim 152, wherein

          said data distribution apparatus provides said second module further storing at least one data among data for verifying if the data has been tampered with for  
25           at least one data of the content data, content key data,



and usage control policy data and signature data for verifying if the data has been certified as legitimate by a predetermined manager to said data processing apparatus.

5           160. A data providing system as set forth in claim 152, wherein

                  said said data processing apparatus determines at least one of the purchase form and the usage form of the distributed content data based on the usage control  
10 policy data and sends log data showing the log of at least one of the purchase form and usage form decided to said management apparatus and

                  said management apparatus performs profit distribution processing for distributing the profit  
15 obtained along with the purchase and usage of the content data in the data processing apparatus to the interested parties of the data providing apparatus and data distribution apparatus based on the received log data.

                  161. A data providing system as set forth in claim  
20 152, wherein

                  said data processing apparatus sends distribution use log data relating to the distribution of the data distribution apparatus to said data distribution apparatus and

25           said data distribution apparatus performs

charge processing relating to that distribution based on the distribution use log data.

162. A data providing system for providing content data from a data providing apparatus to a data distribution apparatus, distributing the content data from said data distribution apparatus to a data processing apparatus, and managing said data providing apparatus, said data distribution apparatus, and said data processing apparatus by a management apparatus, wherein

said management apparatus prepares a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of said content data,

said data providing apparatus provides a first module storing a content file storing the content data encrypted by using said content key data and said key file received from said management apparatus to said data distribution apparatus,

said data distribution apparatus distributes a second module storing said provided content file and said key file to said data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and

5       said data processing apparatus decrypts said  
content key data and said usage control policy data  
stored in said distributed second module and determines  
the handling of said content data stored in said  
distributed second module based on the related decrypted  
usage control policy data.

10       163. A data providing system as set forth in claim  
162, wherein said management apparatus produces signature  
data for verifying the legitimacy of the producer of said  
key file and prepares said key file further storing the  
related signature data.

164. A data providing system as set forth in claim  
162, wherein

15       said data providing apparatus produces said  
content key data and said usage control policy data and  
transmits the same to said management apparatus, and

20       said management apparatus prepares said key  
file based on said received content key data and usage  
control policy data and registers the received content  
key data and usage control policy data.

25       165. A data providing system as set forth in claim  
162, wherein said data providing apparatus produces  
signature data for verifying at least one of the  
legitimacy of a producer and provider of said content  
file and a provider of said key file and distributes said

module further storing said signature data to said data processing apparatus.

166. A data providing system as set forth in claim 162, wherein said data distribution apparatus produces signature data for verifying at least one of the legitimacy of a producer and distributor of said content file and a distributor of said key file and distributes said second module further storing said signature data to said data processing apparatus.

167. A data providing system as set forth in claim 166, wherein said data processing apparatus verifies the signature data stored in said second module to confirm at least one of the legitimacy of a producer and distributor of said content file and a producer and distributor of said key file.

168. A data providing system as set forth in claim 162, wherein said data providing apparatus further stores in said content file expansion use software for expanding the content data when the content data is compressed.

169. A data providing system as set forth in claim 162, wherein said data providing apparatus stores metadata relating to the explanation of the content of the content data in said content file or distributes it separately from the content file to said data processing apparatus.

170. A data providing system as set forth in claim  
162, wherein said data providing apparatus further stores  
in said content file an electronic watermark information  
module including information used for detecting said  
5 electronic watermark information when electronic  
watermark information is buried in said content file.

171. A data providing system as set forth in claim  
162, wherein said management apparatus  
produces said key file storing said content  
10 file data and said usage control policy data encrypted  
using said distribution use key data and

distributes said distribution use key data to  
said data processing apparatus.

172. A data providing system as set forth in claim  
15 171, wherein said management apparatus and said data  
processing apparatus comprise a plurality of distribution  
use key data of defined periods of validity and use  
distribution use key data of corresponding periods.

173. A data providing system as set forth in claim  
20 162, wherein said management apparatus produces said key  
file further storing data describing the grammar of said  
usage policy control data.

174. A data providing system as set forth in claim  
162, wherein  
25 said management apparatus distributes data

showing information for reading the content file and the  
key file, that is, a file reader, to said data processing  
apparatus and

said data processing apparatus reads said  
5 content file and said key file based on the file reader.

175. A data providing system as set forth in claim  
162, wherein

said data providing apparatus distributes data  
showing information for reading the content file and the  
10 key file, that is, a file reader, to said data processing  
apparatus and

said data processing apparatus reads said  
content file and said key file based on the file reader.

176. A data providing system as set forth in claim  
15 165, wherein

said data providing apparatus produces said  
signature data using its own secret key data and

said data processing apparatus verifies the  
legitimacy of said signature data using public key data  
20 corresponding to said secret key data.

177. A data providing system as set forth in claim  
176, wherein

said data providing apparatus distributes said  
module further storing public key certificate data  
25 certifying the legitimacy of said public key data to said

09856276.100201



said data processing apparatus verifies the legitimacy of said signature data using public key data stored in said distributed public key certificate data.

181. A data providing system as set forth in claim  
5 179, wherein

said management apparatus distributes public key certificate data certifying the legitimacy of said public key data to said data processing apparatus and

said data processing apparatus verifies the  
10 legitimacy of said signature data using public key data stored in said distributed public key certificate data.

182. A data providing system as set forth in claim  
162, wherein said data distribution apparatus performs mutual certification with said data processing apparatus,  
15 encrypts said module using session key data obtained by said mutual certification, and sends the encrypted second module to said data processing apparatus.

183. A data providing system as set forth in claim  
182, wherein said data distribution apparatus produces a  
20 storage medium recording said module.

184. A data providing system as set forth in claim  
162, wherein said data processing apparatus determines at least one of a purchase form and a usage form of said content data based on said usage control policy data.

25 185. A data providing system as set forth in claim

09556376-100201  
10200T-9229580



162, wherein said data processing apparatus outputs said encrypted content key data and said encrypted content data to a decryption device.

186. A data providing system as set forth in claim  
5 162, wherein

said data processing apparatus determines at least one of the purchase form and the usage form of the distributed content data based on the usage control policy data and sends log data showing the log of at  
10 least one of the purchase form and usage form decided to said management apparatus, and

said management apparatus performs profit distribution processing for distributing the profit obtained along with the purchase and usage of the content  
15 data in the data processing apparatus to the interested parties of the data providing apparatus and data distribution apparatus based on the received log data.

187. A data providing system as set forth in claim  
186, wherein said management apparatus performs said  
20 profit distribution processing in units of content data.

188. A data providing system as set forth in claim  
162, wherein said data distribution apparatus distributes said second module storing price data showing a price of said content data to said data processing apparatus.

25 189. A data providing system as set forth in claim

186, wherein said management apparatus registers said price data received from said data distribution apparatus.

190. A data providing system as set forth in claim 5 162, wherein said data processing apparatus comprises a module giving resistance to outside monitoring and tampering of the processing content, predetermined data stored in an internal memory, and data being processed.

191. A data providing system as set forth in claim 10 162, wherein

when said first module and said second module store a plurality of content files and a plurality of key files corresponding to the plurality of content files,

said first module and said second module 15 further include data showing the correspondence of the plurality of content files and the corresponding key files.

192. A data providing system as set forth in claim 162, wherein

20 said data providing apparatus distributes a module storing a plurality of said content files and a plurality of key files corresponding to the plurality of content files to said data processing apparatus and

said content files include directory structure 25 data showing the relationship among the plurality of

09856276 100201

content files and the relationship with said key files.

193. A data providing system as set forth in claim 162, wherein said data providing apparatus further comprises a memory circuit for storing said module.

5 194. A data providing system as set forth in claim 193, wherein said data providing apparatus manages said module based on a content identifier uniquely allocated to said content data.

10 195. A data providing system as set forth in claim 194, wherein said management apparatus prepares said key file further storing said content identifier.

15 196. A data providing system as set forth in claim 194, wherein said content identifier is determined uniquely in said content data stored by said data providing apparatus in said memory circuit.

197. A data providing system as set forth in claim 194, wherein said content identifier is determined uniquely globally.

20 198. A data providing system as set forth in claim 194, wherein said data providing apparatus produces said content identifier.

199. A data providing system as set forth in claim 194, wherein said data providing apparatus further comprises a memory circuit for storing said module.

25 200. A data providing system for providing content

09856276 100201

data from a data providing apparatus to a data  
distribution apparatus, distributing the content data  
from said data distribution apparatus to a data  
processing apparatus, and managing said data providing  
5 apparatus, said data distribution apparatus, and said  
data processing apparatus by a management apparatus,  
wherein

said management apparatus prepares a key file  
storing encrypted content key data and encrypted usage  
10 control policy data indicating the handling of said  
content data,

said data providing apparatus provides a first  
module storing a content file containing the content data  
encrypted by using said content key data and a key file  
15 received from said management apparatus to said data  
distribution apparatus,

said data distribution apparatus distributes a  
second module storing said provided content file to said  
data processing apparatus by using a predetermined  
20 communication protocol but in a format not depending upon  
the related communication protocol or recording the same  
on a storage medium, and

said data processing apparatus decrypts said  
content key data and said usage control policy data  
25 stored in said distributed second module and determines

the handling of said content data stored in said distributed second module based on the related decrypted usage control policy data.

201. A data providing system for providing content  
5 data from a data providing apparatus to a first data distribution apparatus and a second data distribution apparatus, distributing the content data from said first data distribution apparatus and said second data distribution apparatus to a data processing apparatus,  
10 and managing said data providing apparatus, said first data distribution apparatus, said second data distribution apparatus, and said data processing apparatus by a management apparatus, wherein

said management apparatus prepares a key file  
15 storing encrypted content key data and encrypted usage control policy data indicating the handling of said content data,

said data providing apparatus provides a first module storing a content file storing the content data  
20 encrypted by using said content key data and said key file received from said management apparatus to said first data distribution apparatus and said second data distribution apparatus,

said first data distribution apparatus  
25 distributes a second module storing said provided content

09856276-100201

file and said key file to said data processing apparatus,  
said second data distribution apparatus  
distributes a third module storing said provided content  
file and said key file to said data processing apparatus,  
5 and

said data processing apparatus decrypts said  
content key data and said usage control policy data  
stored in said distributed second module and said third  
module and determines the handling of said content data  
10 based on the related decrypted usage control policy data.

202. A data providing system as set forth in claim  
201, wherein

said first data distribution apparatus  
distributes said second module storing first price data  
15 showing a price of said content data to said data  
processing apparatus and

said second data distribution apparatus  
distributes said third module storing second price data  
showing a price of content data to said data processing  
20 apparatus.

203. A data providing system for providing first  
content data from a first data providing apparatus to a  
data distribution apparatus, providing second content  
data from a second data providing apparatus to the data  
25 distribution apparatus, distributing the content data

from said data distribution apparatus to a data  
processing apparatus, and managing said first data  
providing apparatus, said second data providing  
apparatus, said data distribution apparatus, and said  
5 data processing apparatus by a management apparatus,  
wherein

said management apparatus prepares a first key  
file storing an encrypted first content key data and an  
encrypted first usage control policy data indicating the  
10 handling of said first content data and a second key file  
storing an encrypted second content key data and an  
encrypted second usage control policy data indicating the  
handling of said second content data,

said first data providing apparatus provides a  
15 first module storing a first content file storing said  
first content data encrypted by using said first content  
key data and said first key file received from said  
management apparatus to said data distribution apparatus,

said second data providing apparatus provides a  
20 second module storing a second content file storing said  
second content data encrypted by using said second  
content key data and said second key file received from  
said management apparatus to said data distribution  
apparatus,

25 said data distribution apparatus distributes a

09856276-100201

third module storing said provided first content file,  
said first key file, said second content file, and said  
second key file to said data processing apparatus, and  
said data processing apparatus decrypts said  
5 first content key data, said second content key data,  
said first usage control policy data, and said second  
usage control policy data stored in said distributed  
third module, determines the handling of said first  
content data based on the related decrypted first usage  
10 control policy data, and determines the handling of said  
second content data based on the related decrypted second  
usage control policy data.

204. A data providing system as set forth in claim  
203, wherein said data distribution apparatus distributes  
15 said third module further storing first price data  
showing a price of said first content data and second  
price data showing a price of said second content data to  
said data processing apparatus.

205. A data providing system for providing content  
20 data from a data providing apparatus to a data  
distribution apparatus, distributing the content data  
from said data distribution apparatus to a data  
processing apparatus, and managing said data providing  
apparatus, said data distribution apparatus, and said  
25 data processing apparatus by a management apparatus,



wherein

said management apparatus prepares a key file  
storing encrypted content key data and encrypted usage  
control policy data indicating the handling of said  
5 content data,

said data providing apparatus individually  
distributes a content file storing the content data  
encrypted by using said content key data and said key  
file received from said management apparatus to said data  
10 distribution apparatus,

said data distribution apparatus individually  
distributes said distributed content file and said key  
file to said data processing apparatus by using a  
predetermined communication protocol but in a format not  
15 depending upon the related communication protocol or by  
recording the same on a storage medium, and

said data processing apparatus decrypts said  
content key data and said usage control policy data  
stored in said distributed key file and determines the  
20 handling of said content data stored in said distributed  
content file based on the related decrypted usage control  
policy data.

206. A data providing system as set forth in claim  
205, wherein said content file and said key file include  
25 data for clearing indicating their mutual correspondence.

09856276 100201



policy data.

208. A data providing system as set forth in claim 207, wherein said content file and said key file include data for clearing indicating their mutual correspondence.

5

209. A data providing system for providing content data from a data providing apparatus to a data distribution apparatus, distributing the content data from said data distribution apparatus to a data processing apparatus, and managing said data providing apparatus, said data distribution apparatus, and said data processing apparatus by a management apparatus, wherein

said management apparatus prepares a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of said content data,

said data providing apparatus provides a first module storing the content data encrypted by using said content key data and said key file received from said management apparatus to said data distribution apparatus,

said data distribution apparatus distributes a second module storing said provided content data and said key file to said data processing apparatus by using a predetermined communication protocol but in a format not

09050275.100201

depending upon the related communication protocol or by recording the same on a storage medium, and

5       said data processing apparatus decrypts said content key data and said usage control policy data stored in said distributed second module and determines the handling of said content data stored in said distributed second module based on the related decrypted usage control policy data.

210. A data providing system for providing content  
10   data from a data providing apparatus to a data distribution apparatus, distributing the content data from said data distribution apparatus to a data processing apparatus, and managing said data providing apparatus, said data distribution apparatus, and said  
15   data processing apparatus by a management apparatus, wherein

      said management apparatus prepares a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of said  
20   content data,

      said data providing apparatus individually distributes the content data encrypted by using said content key data and said key file received from said management apparatus to said data distribution apparatus,

25       said data distribution apparatus individually

09050376-100201

distributes said distributed content data and said key  
file to said data distribution apparatus by using a  
predetermined communication protocol but in a format not  
depending upon the related communication protocol or by  
5 recording the same on a storage medium, and

said data processing apparatus decrypts said  
content key data and said usage control policy data  
stored in said distributed key file and determines the  
handling of said distributed content data based on the  
10 related decrypted usage control policy data.

211. A data providing system for providing content  
data from a data providing apparatus to a data processing  
apparatus, and managing said data providing apparatus and  
said data processing apparatus by a management apparatus,  
15 wherein

said management apparatus prepares a key file  
storing encrypted content key data and encrypted usage  
control policy data indicating the handling of said  
content data and distributes the related prepared key  
20 file to said data processing apparatus,

said data providing apparatus distributes the  
content data encrypted by using said content key data to  
said data distribution apparatus,

said data distribution apparatus distributes  
25 said provided content data to said data processing

apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or by recording the same on a storage medium, and

5           said data processing apparatus decrypts said content key data and said usage control policy data stored in said distributed key file and determines the handling of said distributed content data based on the related decrypted usage control policy data.

10           212. A data providing system for providing content data from a data providing apparatus to a data distribution apparatus, distributing the content data from said data distribution apparatus to a data processing apparatus, and managing said data providing  
15   apparatus, said data distribution apparatus, and said data processing apparatus by a management apparatus, wherein

          said management apparatus provides encrypted content key data and encrypted usage control policy data  
20   indicating the handling of said content data to said data providing apparatus,

          said data providing apparatus individually distributes the content data encrypted by using said content key data and said encrypted content key data and  
25   said encrypted usage control policy data received from

said management apparatus to said data distribution apparatus,

said data distribution apparatus distributes said distributed content data, said encrypted content key data, and said encrypted usage control policy data to said data distribution apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and

said data processing apparatus decrypts said distributed content key data and said usage control policy data and determines the handling of said distributed content data based on the related decrypted usage control policy data.

213. A data providing system for providing content data from a data providing apparatus to a data distribution apparatus, distributing the content data from said data distribution apparatus to a data processing apparatus, and managing said data providing apparatus, said data distribution apparatus, and said data processing apparatus by a management apparatus, wherein

said management apparatus provides encrypted content key data and encrypted usage control policy data indicating the handling of said content data to said data

processing apparatus,

said data providing apparatus provides the  
content data encrypted by using said content key data to  
said data distribution apparatus,

5           said data distribution apparatus distributes  
said distributed provided content data to said data  
processing apparatus by using a predetermined  
communication protocol but in a format not depending upon  
the related communication protocol or recording the same  
10   on a storage medium, and

          said data processing apparatus decrypts said  
distributed content key data and said usage control  
policy data and determines the handling of said  
distributed content data based on the related decrypted  
15   usage control policy data.

214. A data providing system comprising a data  
providing apparatus, a data distribution apparatus, a  
management apparatus, and a data processing apparatus,  
wherein

20           said data providing apparatus provides master  
source data of content to said management apparatus,

          said management apparatus manages said data  
providing apparatus, said data distribution apparatus,  
and said data processing apparatus, encrypts said  
25   provided master source data by using content key data to

09856276-100201



prepare content data, prepares a content file storing the related content data, prepares a key file storing said encrypted content key data and encrypted usage control policy data indicating the handling of said content data, and provides said content file and said key file to said data distribution apparatus,

said data distribution apparatus distributes said provided content file and said key file to said data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and

said data processing apparatus decrypts said content key data and said usage control policy data stored in said distributed key file and determines the handling of the content data stored in said distributed content file based on the related decrypted usage control policy data.

215. A data providing system as set forth in claim 214, wherein

said management apparatus produces a first module storing said content file and said key file and provides the first module to said data distribution apparatus and

said data distribution apparatus produces a

09856276-100204

second file storing said content file and said key file stored in said first module and distributes the second module to said data providing apparatus.

216. A data providing system as set forth in claim 5 214, wherein said management apparatus

comprises at least one database among a database for storing and managing said content file, a database for storing and managing said key file, and a database for storing and managing said usage control 10 policy data and

centrally manages at least one among said content file, said key file, and said usage control policy data by using a content identifier uniquely allocated to said content data.

15 217. A data providing system as set forth in claim 214, wherein said data providing apparatus provides said content key data and said usage control policy data to said management apparatus.

20 218. A data providing system comprising a data providing apparatus, a data distribution apparatus, a management apparatus, and a data processing apparatus, wherein

said data providing apparatus provides master source data of content to said management apparatus,

25 said management apparatus manages said data

09856276-100201

providing apparatus, said data distribution apparatus,  
and said data processing apparatus, encrypts said  
provided master source data by using content key data to  
prepare content data, prepares a content file storing the  
5 related content data, prepares a key file storing said  
encrypted content key data and encrypted usage control  
policy data indicating the handling of said content data,  
and provides said content file to said data distribution  
apparatus and provides said key file to said data  
10 processing apparatus,  
said data distribution apparatus distributes  
said provided content file to said data processing  
apparatus by using a predetermined communication protocol  
but in a format not depending upon the related  
15 communication protocol or recording the same on a storage  
medium, and  
said data processing apparatus decrypts said  
content key data and said usage control policy data  
stored in said provided key file and determines the  
20 handling of the content data stored in said distributed  
content file based on the related decrypted usage control  
policy data.

219. A data providing system comprising a data  
providing apparatus, a data distribution apparatus, a  
25 management apparatus, and a data processing apparatus,

wherein

said data providing apparatus provides a content file storing encrypted content data using content key data to said management apparatus,

5           said management apparatus manages said data providing apparatus, said data distribution apparatus, and said data processing apparatus, prepares a key file storing said encrypted content key data and encrypted usage control policy data indicating the handling of said  
10 content data, and provides said content file provided from said data providing apparatus and said prepared key file to said data distribution apparatus,

          said data distribution apparatus distributes said provided content file and said key file to said data  
15 processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or by recording the same on a storage medium, and

          said data processing apparatus decrypts said  
20 content key data and said usage control policy data stored in said distributed key file and determines the handling of the content data stored in said distributed content file based on the related decrypted usage control policy data.

25           220. A data providing system as set forth in claim

09856276-100201

219, wherein

said management apparatus produces a first module storing said content file and said key file and provides the first module to said data distribution

5 apparatus and

said data distribution apparatus produces a second file storing said content file and said key file stored in said first module and distributes the second module to said data providing apparatus.

10 221. A data providing system as set forth in claim 219, wherein said management apparatus

comprises at least one database among a database for storing and managing said content file, a database for storing and managing said key file, and a  
15 database for storing and managing said usage control policy data and

centrally manages at least one among said content file, said key file, and said usage control policy data by using a content identifier uniquely  
20 allocated to said content data.

222. A data providing system as set forth in claim 219, wherein said data providing apparatus provides said content key data and said usage control policy data to said management apparatus.

25 223. A data providing system comprising a data

09856276-100201

providing apparatus, a data distribution apparatus, a management apparatus, and a data processing apparatus, wherein

said data providing apparatus provides a  
5 content file storing encrypted content data using content key data to said management apparatus,

said management apparatus manages said data providing apparatus, said data distribution apparatus, and said data processing apparatus, prepares a key file  
10 storing said encrypted content key data and encrypted usage control policy data indicating the handling of said content data, provides said content file provided from said data providing apparatus to said data distribution apparatus, and provides said prepared key file to said  
15 data processing apparatus,

said data distribution apparatus distributes said provided content file to said data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related  
20 communication protocol or by recording the same on a storage medium, and

said data processing apparatus decrypts said content key data and said usage control policy data stored in said provided key file and determines the  
25 handling of the content data stored in said distributed

09656276-100001

content file based on the related decrypted usage control policy data.

224. A data providing system comprising a data providing apparatus, a data distribution apparatus, a management apparatus, a database device, and a data processing apparatus, wherein

said data providing apparatus encrypts content data by using content key data, prepares a content file storing the related encrypted content data, and stores the related prepared content file and a key file provided from said management apparatus in said database device,

said management apparatus prepares a key file storing said encrypted content key data and encrypted usage control policy data indicating the handling of said content data and provides the related prepared key file to said data providing apparatus,

said data distribution apparatus distributes said content file and key file obtained from said database device to said data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and

said data processing apparatus decrypts said content key data and said usage control policy data stored in said distributed key file and determines the

09856276-100201

handling of said content data stored in said distributed content file based on the related decrypted usage control policy data.

225. A data providing system as set forth in claim 5 224, wherein said database device centrally manages said stored content file and key file using a content identifier uniquely allocated to said content data.

226. A data providing system as set forth in claim 224, wherein said management apparatus 10 comprises at least one database among a database for storing and managing said key file and a database for storing and managing said usage control policy data and

centrally manages at least one among said key 15 file and said usage control policy data by using a content identifier uniquely allocated to said content data.

227. A data providing system as set forth in claim 224, wherein said data providing apparatus provides said 20 content key data and said usage control policy data to said management apparatus.

228. A data providing system comprising a data providing apparatus, a data distribution apparatus, a management apparatus, a database device, and a data 25 processing apparatus, wherein



said data providing apparatus encrypts content data by using content key data, prepares a content file storing the related encrypted content data, and stores the related prepared content file in said database device,

said management apparatus prepares a key file storing said encrypted content key data and encrypted usage control policy data indicating the handling of said content data and provides the related prepared key file to said data providing apparatus,

said data distribution apparatus distributes said content file obtained from said database device and the key file provided from said data distribution apparatus to said data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and

said data processing apparatus decrypts said content key data and said usage control policy data stored in said distributed key file and determines the handling of said content data stored in said distributed content file based on the related decrypted usage control policy data.

229. A data providing system comprising a data providing apparatus, a data distribution apparatus, a

098556276.100204

management apparatus, a database device, and a data processing apparatus, wherein

said data providing apparatus encrypts content data by using content key data, prepares a content file storing the related encrypted content data, and stores the related prepared content file in said database device,

said management apparatus prepares a key file storing said encrypted content key data and encrypted usage control policy data indicating the handling of said content data and provides the related prepared key file to said data processing apparatus,

said data distribution apparatus distributes said content file obtained from said database device to said data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and

said data processing apparatus decrypts said content key data and said usage control policy data stored in said provided key file and determines the handling of said content data stored in said distributed content file based on the related decrypted usage control policy data.

230. A data providing system comprising a plurality

of data providing apparatuses, a data distribution apparatus, a plurality of management apparatuses, a database device, and a data processing apparatus, wherein

5       said data providing apparatuses encrypt content data by using content key data, prepare content files storing the related encrypted content data, and store the related prepared content files and key files provided from corresponding management apparatuses in said database device,

10               said management apparatuses prepare key files storing said encrypted content key data and encrypted usage control policy data indicating the handling of said content data for the content data provided by corresponding data providing apparatuses and provide the  
15       related prepared key files to corresponding data providing apparatuses,

              said data distribution apparatus distributes said content files and key files obtained from said database device to said data processing apparatus by  
20       using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and

              said data processing apparatus decrypts said content key data and said usage control policy data  
25       stored in said distributed key files and determines the

09856276-100201

handling of said content data stored in said distributed content files based on the related decrypted usage control policy data.

231. A data providing system as set forth in claim 5 230, wherein said database device centrally manages said stored content files and key files using content identifiers uniquely allocated to said content data.

232. A data providing system as set forth in claim 230, wherein said management apparatuses 10 comprise at least one database among a database for storing and managing said key files and a database for storing and managing said usage control policy data and centrally manage at least one among said key 15 files and said usage control policy data by using content identifiers uniquely allocated to said content data provided by said data providing apparatuses in said corresponding data providing apparatuses.

233. A data providing system as set forth in claim 20 230, wherein said data providing apparatuses provide said content key data and said usage control policy data to said management apparatuses.

234. A data providing system comprising a plurality of data providing apparatuses, a data distribution 25 apparatus, a plurality of management apparatuses, a

database device, and a data processing apparatus, wherein

said data providing apparatuses encrypt content data by using content key data, prepare content files storing the related encrypted content data, and store the

5 related prepared content files in said database device,

said management apparatuses prepare key files storing said encrypted content key data and encrypted usage control policy data indicating the handling of said content data for the content data provided by

10 corresponding data providing apparatuses and provide the related prepared key files to said data distribution apparatus,

said data distribution apparatus distributes said content files obtained from said database device and  
15 the key files provided from said management apparatuses to said data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and

20 said data processing apparatus decrypts said content key data and said usage control policy data stored in said distributed key files and determines the handling of said content data stored in said distributed content files based on the related decrypted usage  
25 control policy data.

09955276-100201

235. A data providing system comprising a plurality of data providing apparatuses, a data distribution apparatus, a plurality of management apparatuses, a database device, and a data processing apparatus, wherein

5           said data providing apparatuses encrypt content data by using content key data, prepare content files storing the related encrypted content data, and store the related prepared content files in said database device,

                  said management apparatuses prepare key files  
10   storing said encrypted content key data and encrypted usage control policy data indicating the handling of said content data for the content data provided by corresponding data providing apparatuses and provide the related prepared key files to said data processing  
15   apparatus,

                  said data distribution apparatus distributes said content files obtained from said database device to said data processing apparatus by using a predetermined communication protocol but in a format not depending upon  
20   the related communication protocol or recording the same on a storage medium, and

                  said data processing apparatus decrypts said content key data and said usage control policy data stored in said provided key files and determines the  
25   handling of said content data stored in said distributed

09856276-100201

content files based on the related decrypted usage  
control policy data.

236. A data providing system comprising a plurality  
of data providing apparatuses, a data distribution  
5 apparatus, a plurality of management apparatuses, a  
database device, and a data processing apparatus, wherein  
said data providing apparatuses provide master  
sources of content data to corresponding management  
apparatuses and store content files and key files  
10 received from the related management apparatuses in said  
database,  
said management apparatuses encrypt said master  
sources received from corresponding data providing  
apparatuses by using content key data, prepare content  
15 files storing the related encrypted content data, prepare  
key files storing said encrypted content key data and  
encrypted usage control policy data indicating the  
handling of said content data for the content data  
provided by corresponding data providing apparatuses, and  
20 send said prepared content files and said prepared key  
files to corresponding data providing apparatuses,  
said data distribution apparatus distributes  
said content files and key files obtained from said  
database device to said data processing apparatus by  
25 using a predetermined communication protocol but in a

format not depending upon the related communication  
protocol or by recording the same on a storage medium,  
and

5       said data processing apparatus decrypts said  
content key data and said usage control policy data  
stored in said distributed key files and determines the  
handling of said content data stored in said distributed  
content files based on the related decrypted usage  
control policy data.

10       237. A data providing system as set forth in claim  
236, wherein said database device centrally manages said  
stored content files and key files using content  
identifiers uniquely allocated to said content data.

15       238. A data providing system as set forth in claim  
236, wherein said management apparatuses  
comprise at least one database among a database  
for storing and managing said key files and a database  
for storing and managing said usage control policy data  
and

20       centrally manage at least one among said key  
files and said usage control policy data by using content  
identifiers uniquely allocated to said content data  
provided by said data providing apparatuses in said  
corresponding data providing apparatuses.

25       239. A data providing system as set forth in claim

09856276 100201



236, wherein said data providing apparatuses provide said content key data and said usage control policy data to said management apparatuses.

240. A data providing system comprising a plurality  
5 of data providing apparatuses, a data distribution  
apparatus, a plurality of management apparatuses, a  
database device, and a data processing apparatus, wherein  
said data providing apparatuses provide master  
sources of content data to corresponding management  
10 apparatuses and store content files received from the  
related management apparatuses in said database,  
said management apparatuses encrypt said master  
sources received from corresponding data providing  
apparatuses by using content key data, prepare content  
15 files storing the related encrypted content data, send  
the related prepared content files to said data providing  
apparatuses, prepare key files storing said encrypted  
content key data and encrypted usage control policy data  
indicating the handling of said content data for the  
20 content data provided by corresponding data providing  
apparatuses, and send the related prepared key files  
provided from said management apparatuses to  
corresponding data distribution apparatus,  
said data distribution apparatus distributes  
25 said content files obtained from said database device and

09856276-100201

key files provided from said management apparatuses to  
said data processing apparatus by using a predetermined  
communication protocol but in a format not depending upon  
the related communication protocol or by recording the  
5 same on a storage medium, and

said data processing apparatus decrypts said  
content key data and said usage control policy data  
stored in said distributed key files and determines the  
handling of said content data stored in said distributed  
10 content files based on the related decrypted usage  
control policy data.

241. A data providing system comprising a plurality  
of data providing apparatuses, a data distribution  
apparatus, a plurality of management apparatuses, a  
15 database device, and a data processing apparatus, wherein

said data providing apparatuses provide master  
sources of content data to corresponding management  
apparatuses and store content files received from the  
related management apparatuses in said database,

20 said management apparatuses encrypt said master  
sources received from corresponding data providing  
apparatuses by using content key data, prepare content  
files storing the related encrypted content data, send  
the related prepared content files to said data providing  
25 apparatuses, prepare key files storing said encrypted

09855276-10001

content key data and encrypted usage control policy data  
indicating the handling of said content data for the  
content data provided by corresponding data providing  
apparatuses, and send the related prepared key files to  
5 said data processing apparatus,

said data distribution apparatus distributes  
said content files obtained from said database device to  
said data processing apparatus by using a predetermined  
communication protocol but in a format not depending upon  
10 the related communication protocol or by recording the  
same on a storage medium, and

said data processing apparatus decrypts said  
content key data and said usage control policy data  
stored in said distributed key files and determines the  
15 handling of said content data stored in said provided  
content files based on the related decrypted usage  
control policy data.

242. A data providing system comprising a data  
providing apparatus, a data distribution apparatus, and a  
20 data processing apparatus, wherein

said data providing apparatus provides a first  
module storing content data encrypted by using content  
key data, said encrypted content key data, and encrypted  
usage control policy data indicating the handling of said  
25 content data to said data distribution apparatus,

09556276-100201

performs charge processing in units of the content data based on log data received from said data processing apparatus, and performs a profit distribution processing for distributing the profit paid by interested parties of  
5 said data processing apparatus to interested parties of the related data providing apparatus and interested parties of said data distribution apparatus,

said data distribution apparatus distributes a second module storing said encrypted content data,  
10 content key data, and usage control policy data stored in said provided first module to said data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or by recording the same on a  
15 storage medium, and

said data processing apparatus decrypts said content key data and said usage control policy data stored in said distributed module, determines the handling of said content data based on the related  
20 decrypted usage control policy data, prepares the log data for the handling of the related content data, and sends the related log data to said data providing apparatus.

243. A data providing system as set forth in claim  
25 242, wherein

09856275-100201

said data processing apparatus sends data  
distribution use apparatus use log data relating to the  
distribution service of the content data performed by the  
data distribution apparatus to said data distribution  
5 apparatus and

said data distribution apparatus performs  
charge processing based on that data distribution  
apparatus use log data.

244. A data providing system comprising a data  
10 providing apparatus, a data distribution apparatus, and a  
management apparatus, wherein

said data providing apparatus provides content  
data,

said data distribution apparatus distributes  
15 said content file provided from said data providing  
apparatus or a content file in accordance with the  
content data provided by said data providing apparatus  
provided from said management apparatus to said data  
processing apparatus, and

20 said data processing apparatus decrypts the  
usage control policy data stored in a key file received  
from said data distribution apparatus or said management  
apparatus, determines the handling of said content data  
stored in the content file received from said data  
25 distribution apparatus or said management apparatus based

09855276-100201

on the related decrypted usage control policy data, and  
further distributes said content file and key file  
received from said data distribution apparatus or said  
management apparatus to the other data processing  
5 apparatus.

245. A data providing method for distributing  
content data from a data providing apparatus to a data  
processing apparatus, comprising the steps of

10 distributing a module storing the content data  
encrypted by using content key data, said encrypted  
content key data, and encrypted usage control policy data  
indicating the handling of said content data from said  
data providing apparatus to said data processing  
apparatus by using a predetermined communication protocol  
15 but in a format not depending upon the related  
communication protocol or recording the same on a storage  
medium, and

in said data processing apparatus, decrypting  
said content key data and said usage control policy data  
20 stored in said distributed module and determining the  
handling of said content data based on the related  
decrypted usage control policy data.

246. A data providing method for distributing  
content data from a data providing apparatus to a data  
25 processing apparatus and managing said data providing

090506276.100201



apparatus and said data processing apparatus by a  
management apparatus, comprising the steps of,

in said management apparatus, preparing a key  
file storing encrypted content key data and encrypted  
5 usage control policy data indicating the handling of said  
content data,

in said data providing apparatus, distributing  
a module storing a content file containing the content  
data encrypted by using said content key data and a key  
10 file received from said management apparatus to said data  
processing apparatus by using a predetermined  
communication protocol but in a format not depending upon  
the related communication protocol or recording the same  
on a storage medium, and

15 in said data processing apparatus, decrypting  
said content key data and said usage control policy data  
stored in said distributed module and determining the  
handling of said content data based on the related  
decrypted usage control policy data.

20 248. A data providing method for distributing  
content data from a data providing apparatus to a data  
processing apparatus and managing said data providing  
apparatus and said data processing apparatus by a  
management apparatus, comprising the steps of,

25 in said management apparatus, preparing a key



file storing encrypted content key data and encrypted  
usage control policy data indicating the handling of said  
content data,

5 distributing the related prepared key file from  
said management apparatus to said data providing  
apparatus, and

10 individually distributing a content file  
storing the content data encrypted by using said content  
key data and said key file distributed from said  
management apparatus from said data providing apparatus  
to said data processing apparatus by using a  
predetermined communication protocol but in a format not  
depending upon the related communication protocol or  
recording the same on a storage medium, and

15 in said data processing apparatus, decrypting  
said content key data and said usage control policy data  
stored in said distributed key file and determining the  
handling of the content data stored in said distributed  
content file based on the related decrypted usage control  
20 policy data.

249. A data providing method for distributing  
content data from a data providing apparatus to a data  
processing apparatus and managing said data providing  
apparatus and said data processing apparatus by a  
25 management apparatus, comprising the steps of,

in said management apparatus, preparing a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of said content data,

5 distributing the related prepared key file from said management apparatus to said data processing apparatus, and

distributing a content file storing the content data encrypted by using said content key data from said data providing apparatus to said data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and

10

15 in said data processing apparatus, decrypting said content key data and said usage control policy data stored in said distributed key file and determining the handling of the content data stored in said distributed content file based on the related decrypted usage control policy data.

20

250. A data providing method for distributing content data from a data providing apparatus to a data processing apparatus and managing said data providing apparatus and said data processing apparatus by a management apparatus, comprising the steps of,

25

09656276-100201

in said management apparatus, preparing a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of said content data,

5 in said data providing apparatus, distributing a module storing the content data encrypted by using said content key data and said key file received from said management apparatus to said data processing apparatus by using a predetermined communication protocol but in a  
10 format not depending upon the related communication protocol or recording the same on a storage medium, and

in said data processing apparatus, decrypting said content key data and said usage control policy data stored in said distributed module and determining the  
15 handling of said content data based on the related decrypted usage control policy data.

251. A data providing method for distributing content data from a data providing apparatus to a data processing apparatus and managing said data providing  
20 apparatus and said data processing apparatus by a management apparatus, comprising the steps of,

in said management apparatus, preparing a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of said  
25 content data,

in said data providing apparatus, individually  
distributing the content data encrypted by using said  
content key data and said key file received from said  
management apparatus to said data processing apparatus by  
5 using a predetermined communication protocol but in a  
format not depending upon the related communication  
protocol or recording the same on a storage medium, and

in said data processing apparatus, decrypting  
said content key data and said usage control policy data  
10 stored in said distributed key file and determining the  
handling of said distributed content data based on the  
related decrypted usage control policy data.

252. A data providing method for distributing  
content data from a data providing apparatus to a data  
15 processing apparatus and managing said data providing  
apparatus and said data processing apparatus by a  
management apparatus, comprising the steps of,

in said management apparatus, preparing a key  
file storing encrypted content key data and encrypted  
20 usage control policy data indicating the handling of said  
content data and distributing the related prepared key  
file to said data processing apparatus, in said data  
providing apparatus,

distributing the content data encrypted by  
25 using said content key data to said data processing

09856276.100201

apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and

5                   in said data processing apparatus, decrypting said content key data and said usage control policy data stored in said distributed key file and determining the handling of said distributed content data based on the related decrypted usage control policy data.

10               253. A data providing method for distributing content data from a data providing apparatus to a data processing apparatus and managing said data providing apparatus and said data processing apparatus by a management apparatus, comprising the steps of,

15                   in said management apparatus, preparing encrypted content key data and encrypted usage control policy data indicating the handling of said content data,

                  in said data providing apparatus, individually distributing the content data encrypted by using said  
20   content key data and said encrypted content key data and said encrypted usage control policy data received from said management apparatus to said data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related  
25   communication protocol or recording the same on a storage

medium, and

in said data processing apparatus, decrypting  
said distributed content key data and said usage control  
policy data and determining the handling of the content  
5 data stored in said distributed content file based on the  
related decrypted usage control policy data.

254. A data providing method for distributing  
content data from a data providing apparatus to a data  
processing apparatus and managing said data providing  
10 apparatus and said data processing apparatus by a  
management apparatus, comprising the steps of,

in said management apparatus, preparing  
encrypted content key data and encrypted usage control  
policy data indicating the handling of said content data  
15 and distributing the same to said data processing  
apparatus,

in said data providing apparatus, distributing  
the content data encrypted by using said content key data  
to said data processing apparatus by using a  
20 predetermined communication protocol but in a format not  
depending upon the related communication protocol or  
recording the same on a storage medium, and

in said data processing apparatus, decrypting  
said distributed content key data and said usage control  
25 policy data and determining the handling of said

distributed content data based on the related decrypted usage control policy data.

255. A data providing method using a data providing apparatus, a data distribution apparatus, and a data processing apparatus, comprising the steps of

5 providing a first module storing content data encrypted by using content key data, encrypted said content key data, and encrypted usage control policy data indicating the handling of said content data from said data providing apparatus to said data distribution apparatus,

10

distributing a second module storing said encrypted content data, content key data, and the usage control policy data stored in said provided said first module from said data distribution apparatus to said data processing apparatus by using said content key data to said data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and

15

20

in said data processing apparatus, decrypting said content key data and said usage control policy data stored in said distributed second module and determining the handling of said content data based on the related decrypted usage control policy data.

25

FOUO 9295360

256. A data providing method for providing content data from a data providing apparatus to a data distribution apparatus, distributing the content data from said data distribution apparatus to a data processing apparatus, and managing said data providing apparatus, said data distribution apparatus, and said data processing apparatus by a management apparatus, comprising the steps of,

in said management apparatus, preparing a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of said content data,

distributing the related prepared key file from said management apparatus to said data providing apparatus,

providing a first module storing a content file storing the content data encrypted by using said content key data and said key file received from said management apparatus from said data providing apparatus to said data distribution apparatus, and

distributing a second module storing said provided content file and said key file from said data distribution apparatus to said data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication



protocol or recording the same on a storage medium, and

in said data processing apparatus, decrypting  
said content key data and said usage control policy data  
stored in said distributed second module and determining  
5 the handling of said content data stored in said  
distributed second module based on the related decrypted  
usage control policy data.

257. A data providing method for providing content  
data from a data providing apparatus to a data  
10 distribution apparatus, distributing the content data  
from said data distribution apparatus to a data  
processing apparatus, and managing said data providing  
apparatus, said data distribution apparatus and said data  
processing apparatus by a management apparatus,  
15 comprising the steps of,

in said management apparatus, preparing a key  
file storing encrypted content key data and encrypted  
usage control policy data indicating the handling of said  
content data,

20 in said data providing apparatus, providing a  
first module storing a content file containing the  
content data encrypted by using said content key data and  
a key file received from said management apparatus to  
said data distribution apparatus,

25 in said data distribution apparatus,

09856276 100204  
distributing a second module storing said provided  
content file to said data processing apparatus by using a  
predetermined communication protocol but in a format not  
depending upon the related communication protocol or  
5 recording the same on a storage medium, and

in said data processing apparatus, decrypting  
said content key data and said usage control policy data  
stored in said distributed second module and determining  
the handling of said content data stored in said  
10 distributed second module based on the related decrypted  
usage control policy data.

258. A data providing method for providing content  
data from a data providing apparatus to a data  
distribution apparatus, distributing the content data  
15 from said data distribution apparatus to a data  
processing apparatus, and managing said data providing  
apparatus, said data distribution apparatus, and said  
data processing apparatus by a management apparatus,  
comprising the steps of,

20 in said management apparatus, preparing a key  
file storing encrypted content key data and encrypted  
usage control policy data indicating the handling of said  
content data,

distributing said prepared key file from said  
25 management apparatus to said data providing apparatus,

individually providing a content file storing  
the content data encrypted by using said content key data  
and said key file received from said management apparatus  
from said data providing apparatus to said data  
5 distribution apparatus by using a predetermined  
communication protocol but in a format not depending upon  
the related communication protocol or recording the same  
on a storage medium, and

individually distributing said distributed  
10 content file and said key file from said data  
distribution apparatus to said data distribution  
apparatus, and

in said data processing apparatus, decrypting  
said content key data and said usage control policy data  
15 stored in said distributed key file and determining the  
handling of the content data stored in said distributed  
content file based on the related decrypted usage control  
policy data.

259. A data providing method for providing content  
20 data from a data providing apparatus to a data  
distribution apparatus and managing said data providing  
apparatus and said data processing apparatus by a  
management apparatus, comprising the steps of,

in said management apparatus, preparing a key  
25 file storing encrypted content key data and encrypted

usage control policy data indicating the handling of said content data,

distributing the related prepared key file from said management apparatus to said data processing

5 apparatus,

providing a content file storing the content data encrypted by using said content key data from said data providing apparatus to said data distribution apparatus,

10 distributing said provided content file from said data distribution apparatus to said data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage  
15 medium, and

in said data processing apparatus, decrypting said content key data and said usage control policy data stored in said distributed key file and determining the handling of the content data stored in said distributed  
20 content file based on the related decrypted usage control policy data.

260. A data providing method for providing content data from a data providing apparatus to a data distribution apparatus, distributing the content data  
25 from said data distribution apparatus to a data

00556376-10001  
FO2007929880

processing apparatus, and managing said data providing  
apparatus, said data distribution apparatus, and said  
data processing apparatus by a management apparatus,  
comprising the steps of,

5           in said management apparatus, preparing a key  
file storing encrypted content key data and encrypted  
usage control policy data indicating the handling of said  
content data,

in said data providing apparatus, providing a  
10 first module storing the content data encrypted by using  
said content key data and said key file received from  
said management apparatus to said data distribution  
apparatus,

in said data distribution apparatus,  
15 distributing a second module storing said provided  
content data and said key file to said data processing  
apparatus by using a predetermined communication protocol  
but in a format not depending upon the related  
communication protocol or recording the same on a storage  
20 medium, and

in said data processing apparatus, decrypting  
said content key data and said usage control policy data  
stored in said distributed second module and determining  
the handling of said content data stored in said  
25 distributed second module based on the related decrypted

usage control policy data.

261. A data providing method for providing content data from a data providing apparatus to a data distribution apparatus, distributing the content data from said data distribution apparatus to a data processing apparatus, and managing said data providing apparatus, said data distribution apparatus, and said data processing apparatus by a management apparatus, comprising the steps of,

10                   in said management apparatus, preparing a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of said content data,

15                   in said data providing apparatus, individually providing the content data encrypted by using said content key data and said key file received from said management apparatus to said data distribution apparatus,

20                   in said data distribution apparatus, individually distributing said distributed content data and said key file to said data distribution apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage medium, and

25                   in said data processing apparatus, decrypting said content key data and said usage control policy data

09556276-10001  
FOUO 929860

stored in said distributed key file and determining the handling of said distributed content data based on the related decrypted usage control policy data.

262. A data providing method for distributing
- 5 content data from a data providing apparatus to a data processing apparatus and managing said data providing apparatus and said data processing apparatus by a management apparatus, comprising the steps of,
- 10 in said management apparatus, preparing a key file storing encrypted content key data and encrypted usage control policy data indicating the handling of said content data and distributing the related prepared key file to said data processing apparatus, in said data providing apparatus,
- 15 providing the content data encrypted by using said content key data to said data distribution apparatus,
- in said data distribution apparatus, distributing said provided content data to said data processing apparatus, and
- 20 in said data processing apparatus, decrypting said content key data and said usage control policy data stored in said distributed key file and determining the handling of said distributed content data based on the related decrypted usage control policy data.
- 25

263. A data providing method for providing content data from a data providing apparatus to a data distribution apparatus, distributing the content data from said data distribution apparatus to a data processing apparatus, and managing said data providing apparatus, said data distribution apparatus, and said data processing apparatus by a management apparatus, comprising the steps of,

in said management apparatus, providing encrypted content key data and encrypted usage control policy data indicating the handling of said content data to said data providing apparatus,

in said data providing apparatus, individually distributing the content data encrypted by using said content key data and said encrypted content key data and said encrypted usage control policy data received from said management apparatus to said data distribution apparatus,

in said data distribution apparatus, individually distributing said distributed content data, said encrypted content key, data, and said encrypted usage control policy data to said data distribution apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or recording the same on a storage



medium, and

in said data processing apparatus, decrypting  
said distributed content key data and said usage control  
policy data and determining the handling of said

5 distributed content data based on the related decrypted  
usage control policy data.

264. A data providing method for providing content  
data from a data providing apparatus to a data  
distribution apparatus, distributing the content data  
10 from said data distribution apparatus to a data  
processing apparatus, and managing said data providing  
apparatus, said data distribution apparatus, and said  
data processing apparatus by a management apparatus,  
comprising the steps of,

15 in said management apparatus, distributing  
encrypted content key data and encrypted usage control  
policy data indicating the handling of said content data  
to said data processing apparatus,

in said data providing apparatus, providing the  
20 content data encrypted by using said content key data to  
said data distribution apparatus,

in said data distribution apparatus,  
distributing said provided content data to said data  
processing apparatus by using a predetermined  
25 communication protocol but in a format not depending upon

the related communication protocol by recording the same  
on a storage medium, and

in said data processing apparatus, decrypting  
said distributed content key data and said usage control  
5 policy data and determining the handling of said  
distributed content data based on the related decrypted  
usage control policy data.

265. A data providing method using a data providing  
apparatus, a data distribution apparatus, a management  
10 apparatus, and a data processing apparatus, wherein  
said data providing apparatus provides master  
source data of content to said management apparatus,  
said management apparatus manages said data  
providing apparatus, said data distribution apparatus,  
15 and said data processing apparatus, encrypts said  
provided master source data by using content key data to  
prepare content data, prepares a content file storing the  
related content data, prepares a key file storing said  
encrypted content key data and encrypted usage control  
20 policy data indicating the handling of said content data,  
and provides said content file and said key file to said  
data distribution apparatus,  
said data distribution apparatus distributes  
said provided content file and said key file to said data  
25 processing apparatus by using a predetermined

09856276, 100201

communication protocol but in a format not depending upon the related communication protocol or by recording the same on a storage medium, and

5       said data processing apparatus decrypts said content key data and said usage control policy data stored in said distributed key file and determines the handling of said content data stored in said distributed content file based on the related decrypted usage control policy data.

10       266. A data providing method using a data providing apparatus, a data distribution apparatus, a management apparatus, and a data processing apparatus, wherein

      said data providing apparatus provides master source data of content to said management apparatus,

15       said management apparatus manages said data providing apparatus, said data distribution apparatus, and said data processing apparatus, encrypts said provided master source data by using content key data to prepare content data, prepares a content file storing the  
20       related content data, prepares a key file storing said encrypted content key data and encrypted usage control policy data indicating the handling of said content data, and provides said content file to said data distribution apparatus and provides said key file to said data  
25       processing apparatus,

09856276 "100201

said data distribution apparatus distributes  
said provided content file to said data processing  
apparatus by using a predetermined communication protocol  
but in a format not depending upon the related  
5 communication protocol or by recording the same on a  
storage medium, and

said data processing apparatus decrypts said  
content key data and said usage control policy data  
stored in said provided key file and determines the  
10 handling of said content data stored in said distributed  
content file based on the related decrypted usage control  
policy data.

267. A data providing method using a data providing  
apparatus, a data distribution apparatus, a management  
15 apparatus, and a data processing apparatus, wherein

said data providing apparatus provides a  
content file storing encrypted content data using content  
key data to said management apparatus,

said management apparatus manages said data  
20 providing apparatus, said data distribution apparatus,  
and said data processing apparatus, prepares a key file  
storing said encrypted content key data and encrypted  
usage control policy data indicating the handling of said  
content data, and provides said content file provided  
25 from said data providing apparatus and said prepared key

09856276-100201

file to said data distribution apparatus,

said data distribution apparatus distributes  
said provided content file and said key file to said data  
processing apparatus by using a predetermined

5 communication protocol but in a format not depending upon  
the related communication protocol or by recording the  
same on a storage medium, and

said data processing apparatus decrypts said  
content key data and said usage control policy data  
10 stored in said distributed key file and determines the  
handling of the content data stored in said distributed  
content file based on the related decrypted usage control  
policy data.

268. A data providing method using a data providing  
15 apparatus, a data distribution apparatus, a management  
apparatus, and a data processing apparatus, wherein

said data providing apparatus provides a  
content file storing encrypted content data using content  
key data to said management apparatus,

20 said management apparatus manages said data  
providing apparatus, said data distribution apparatus,  
and said data processing apparatus, prepares a key file.  
storing said encrypted content key data and encrypted  
usage control policy data indicating the handling of said  
25 content data, provides said content file provided from

said data providing apparatus to said data distribution apparatus and provides said prepared key file to said data processing apparatus,

5           said data distribution apparatus distributes said provided content file to said data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or by recording the same on a storage medium, and

10           said data processing apparatus decrypts said content key data and said usage control policy data stored in said provided key file and determines the handling of the content data stored in said distributed content file based on the related decrypted usage control  
15 policy data.

269. A data providing method using a data providing apparatus, a data distribution apparatus, a management apparatus, a database device, and a data processing apparatus, wherein

20           said data providing apparatus encrypts content data by using content key data, prepares a content file storing the related encrypted content data, and stores the related prepared content file and a key file provided from said management apparatus in said database device,

25           said management apparatus prepares a key file

storing said encrypted content key data and encrypted usage control policy data indicating the handling of said content data and provides the related prepared key file to said data providing apparatus,

5           said data distribution apparatus distributes said content file and key file obtained from said database device to said data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication  
10 protocol or by recording the same on a storage medium, and

          said data processing apparatus decrypts said content key data and said usage control policy data stored in said distributed key file and determines the  
15 handling of said content data stored in said distributed content file based on the related decrypted usage control policy data.

270. A data providing method using a data providing apparatus, a data distribution apparatus, a management  
20 apparatus, a database device, and a data processing apparatus, wherein

          said data providing apparatus encrypts content data by using content key data, prepares a content file storing the related encrypted content data, and stores  
25 the related prepared content file in said database

device,

said management apparatus prepares a key file storing said encrypted content key data and encrypted usage control policy data indicating the handling of said content data and provides the related prepared key file to said data distribution apparatus,

said data distribution apparatus distributes said content file obtained from said database device and the key file provided from said data distribution apparatus to said data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or by recording the same on a storage medium, and

said data processing apparatus decrypts said content key data and said usage control policy data stored in said distributed key file and determines the handling of said content data stored in said distributed content file based on the related decrypted usage control policy data.

271. A data providing method using a data providing apparatus, a data distribution apparatus, a management apparatus, a database device, and a data processing apparatus, wherein

said data providing apparatus encrypts content data by using content key data, prepares a content file



storing the related encrypted content data, and stores the related prepared content file in said database device,

5       said management apparatus prepares a key file storing said encrypted content key data and encrypted usage control policy data indicating the handling of said content data and provides the related prepared key file to said data processing apparatus,

10       said data distribution apparatus distributes said content file obtained from said database device to said data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or by recording the same on a storage medium, and

15       said data processing apparatus decrypts said content key data and said usage control policy data stored in said provided key file and determines the handling of said content data stored in said distributed content file based on the related decrypted usage control  
20   policy data.

272. A data providing method using a plurality of data providing apparatuses, a data distribution apparatus, a plurality of management apparatuses, a database device, and a data processing apparatus, wherein

25       said data providing apparatuses encrypt content

data by using content key data, prepare content files storing the related encrypted content data, and store the related prepared content files and key files provided from corresponding management apparatuses in said

5 database device,

said management apparatuses prepare key files storing said encrypted content key data and encrypted usage control policy data indicating the handling of said content data for the content data provided by

10 corresponding data providing apparatuses and provide the related prepared key files to corresponding data providing apparatuses,

said data distribution apparatus distributes said content files and key files obtained from said  
15 database device to said data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or by recording the same on a storage medium, and

20 said data processing apparatus decrypts said content key data and said usage control policy data stored in said distributed key files and determines the handling of said content data stored in said distributed content files based on the related decrypted usage  
25 control policy data.

09856276.100201

273. A data providing method using a plurality of data providing apparatuses, a data distribution apparatus, a plurality of management apparatuses, a database device, and a data processing apparatus, wherein

5           said data providing apparatuses encrypt content data by using content key data, prepare content files storing the related encrypted content data, and store the related prepared content files in said database device,

          said management apparatuses prepare key files  
10       storing said encrypted content key data and encrypted usage control policy data indicating the handling of said content data for the content data provided by corresponding data providing apparatuses and provide the related prepared key files to said data distribution

15       apparatus,

          said data distribution apparatus distributes said content files obtained from said database device and the key files provided from said management apparatuses to said data processing apparatus by using a  
20       predetermined communication protocol but in a format not depending upon the related communication protocol or by recording the same on a storage medium, and

          said data processing apparatus decrypts said content key data and said usage control policy data  
25       stored in said distributed key files and determines the

09856276-100201

handling of said content data stored in said distributed content files based on the related decrypted usage control policy data.

274. A data providing method using a plurality of  
5 data providing apparatuses, a data distribution apparatus, a plurality of management apparatuses, a database device, and a data processing apparatus, wherein  
said data providing apparatuses encrypt content data by using content key data, prepare content files  
10 storing the related encrypted content data, and store the related prepared content files in said database device,  
said management apparatuses prepare key files storing said encrypted content key data and encrypted usage control policy data indicating the handling of said  
15 content data for the content data provided by corresponding data providing apparatuses and provide the related prepared key files to said data processing apparatus,  
said data distribution apparatus distributes  
20 said content files obtained from said database device to said data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or by recording the same on a storage medium, and  
25 said data processing apparatus decrypts said

content key data and said usage control policy data  
stored in said provided key files and determines the  
handling of said content data stored in said distributed  
content files based on the related decrypted usage  
5 control policy data.

275. A data providing method using a plurality of  
data providing apparatuses, a data distribution  
apparatus, a plurality of management apparatuses, a  
database device, and a data processing apparatus, wherein  
10 said data providing apparatuses provide master  
sources of content data to corresponding management  
apparatuses and store content files and key files  
received from the related management apparatuses in said  
database,

15 said management apparatuses encrypt said master  
sources received from corresponding data providing  
apparatuses by using content key data, prepare content  
files storing the related encrypted content data, prepare  
key files storing said encrypted content key data and  
20 encrypted usage control policy data indicating the  
handling of said content data for the content data  
provided by corresponding data providing apparatuses, and  
send said prepared content files and said prepared key  
files to corresponding data providing apparatuses,

25 said data distribution apparatus distributes

09856276.100201

5

10

15

20

25

apparatuses, prepare key files storing said encrypted content key data and encrypted usage control policy data indicating the handling of said content data for the content data provided by corresponding data providing apparatuses, and send the related prepared key files to corresponding data distribution apparatus,

said data distribution apparatus distributes said content files obtained from said database device and the key files provided from said management apparatuses to said data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or by recording the same on a storage medium, and

said data processing apparatus decrypts said content key data and said usage control policy data stored in said distributed key files and determines the handling of the content data stored in said distributed content files based on the related decrypted usage control policy data.

277. A data providing method using a plurality of data providing apparatuses, a data distribution apparatus, a plurality of management apparatuses, a database device, and a data processing apparatus, wherein

said data providing apparatuses provide master sources of content data to corresponding management

09856276.100201

apparatuses and store content files received from the related management apparatuses in said database,

5       said management apparatuses encrypt said master sources received from corresponding data providing apparatuses by using content key data, prepare content files storing the related encrypted content data, send the related prepared content files to said data providing apparatuses, prepare key files storing said encrypted content key data and encrypted usage control policy data  
10       indicating the handling of said content data for the content data provided by corresponding data providing apparatuses, and provide the related prepared key files to said data processing apparatus,

15       said data distribution apparatus distributes said content files obtained from said database device to said data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or by recording the same on a storage medium, and

20       said data processing apparatus decrypts said content key data and said usage control policy data stored in said provided key files and determines the handling of the content data stored in said distributed content files based on the related decrypted usage  
25       control policy data.

09050276 100201



278. A data providing method using a data providing apparatus, a data distribution apparatus, and a data processing apparatus, wherein

5       said data providing apparatus provides a first  
module storing content data encrypted by using content  
key data, said encrypted content key data, and encrypted  
usage control policy data indicating the handling of said  
content data to said data distribution apparatus,  
10       performs charge processing in units of the content data  
based on log data received from said data processing  
apparatus, performs profit distribution processing for  
distributing the profit paid by interested parties of  
said data processing apparatus to interested parties of  
the related data providing apparatus and interested  
15       parties of said data distribution apparatus,

      said data distribution apparatus distributes a  
second module storing said encrypted content data,  
content key data and usage control policy data stored in  
said provided first module to said data processing  
20       apparatus by using a predetermined communication protocol  
but in a format not depending upon the related  
communication protocol or by recording the same on a  
storage medium, and

      said data processing apparatus decrypts said  
25       content key data and said usage control policy data

stored in said distributed module, determines the  
handling of said content data based on the related  
decrypted usage control policy data, prepares the log  
data for the handling of the related content data and  
5 sends the related log data to said data providing  
apparatus.

279. A data providing method using a data providing  
apparatus, a data distribution apparatus, a data  
processing apparatus, and a management apparatus, wherein  
10 said data providing apparatus provides content  
data,

said data distribution apparatus distributes  
said content file provided from said data providing  
apparatus or a content file in accordance with the  
15 content data provided by said data providing apparatus  
received from said management apparatus to said data  
processing apparatus, and

said data processing apparatus decrypts the  
usage control policy data stored in the key file received  
20 from said data distribution apparatus or said management  
apparatus, determines the handling of said content data  
stored in the content file received from said data  
distribution apparatus or said management apparatus based  
on the related decrypted usage control policy data, and  
25 further distributes said content file and key file

09856276.100201

received from said data distribution apparatus or said management apparatus to the other data processing apparatus.

280. A data providing system for distributing  
5 content data from a data providing apparatus to a data processing apparatus, wherein

10 said data providing apparatus distributes a module storing content data encrypted by using content key data, said encrypted content key data, and encrypted usage control policy data indicating the handling of said content data in a format not depending upon at least one among existence of a compression of said content data, a compression method, a method of said encryption, and parameters of a signal giving the content data to said  
15 data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or by recording the same on a storage medium, and

20 said data processing apparatus decrypts said content key data and said usage control policy data stored in said distributed module and determines the handling of said content data based on the related decrypted usage control policy data.

281. A data providing system as set forth in claim  
25 280, wherein

09855276.100201

said data providing apparatus distributes said module further storing a certification data of itself in a format not depending upon the method of producing said certification data.

5           282. A data providing system comprising a data providing apparatus, a data distribution apparatus, and a data processing apparatus, wherein

              said data providing apparatus distributes a first module storing content data encrypted by using  
10   content key data, said encrypted content key data, and encrypted usage control policy data indicating the handling of said content data in a format not depending upon at least one among existence of compression of said content data, a compression method, a method of said  
15   encryption, and parameters of a signal giving the content data to said data distribution apparatus,

              said data distribution apparatus distributes a second module storing said encrypted content data, content key data, and the usage control policy data  
20   stored in said provided first module to said data processing apparatus by using a predetermined communication protocol but in a format not depending upon the related communication protocol or by recording the same on a storage medium, and

25           said data processing apparatus decrypts said

09556276 100201

content key data and said usage control policy data stored in said distributed second module and determines the handling of said content data based on the related decrypted usage control policy data.

5           283. A data providing system as set forth in claim 282, wherein said data providing apparatus provides said first module further storing its own signature data in a format not depending upon the method preparation of the signature data to said data distribution apparatus.

10           284. A data providing system comprising a data providing apparatus, a data distribution apparatus, and a data processing apparatus, wherein

              said data providing apparatus distributes a first module storing content data encrypted by using  
15   content key data, said encrypted content key data, and encrypted usage control policy data indicating the handling of said content data to said data distribution apparatus,

              said data distribution apparatus encrypts a  
20   plurality of second modules storing said encrypted content data, content key data, and the usage control policy data stored in said provided first module by using a common key obtained by mutual certification with said data processing apparatus, and then distributes the same  
25   to said data processing apparatus by using a

09855276.100201

predetermined communication protocol but in a format not depending upon the related communication protocol, and

5       said data processing apparatus comprises a first processing circuit for decrypting said distributed plurality of second modules by using said common key, selecting a single or a plurality of second modules from among the related decrypted plurality of second modules, and performing charge processing with respect to a distribution service of said second modules and a tamper  
10   resistant second processing circuit receiving said selected said second modules, decrypting said content key data and said usage control policy data stored in the related second modules, and determining the handling of said content data based on the related decrypted usage  
15   control policy data.

285. A data providing system as set forth in claim 284, wherein

20       said first processing circuit produces data distribution use apparatus use log data relating to the distribution service of the second module performed by the data distribution apparatus to said data distribution apparatus and

25       said data distribution apparatus performs charge processing based on that data distribution apparatus use log data.

09856276 100201

286. A data providing system as set forth in claim  
284,

further comprising a management apparatus for  
managing said data providing apparatus, said data  
5 distribution apparatus, and said data processing  
apparatus, wherein

said second processing circuit determines the  
handling of said content data, prepares usage log data in  
accordance with the determination, and sends the usage  
10 log data to said management apparatus, and

said management apparatus performs profit  
distribution processing for distributing the profit  
relating to the content data paid by an interested party  
of the data processing apparatus based on the usage log  
15 data to interested parties of the data providing  
apparatus and the data distribution apparatus based on  
the usage log data.

00856276 "100201"

FIG.1

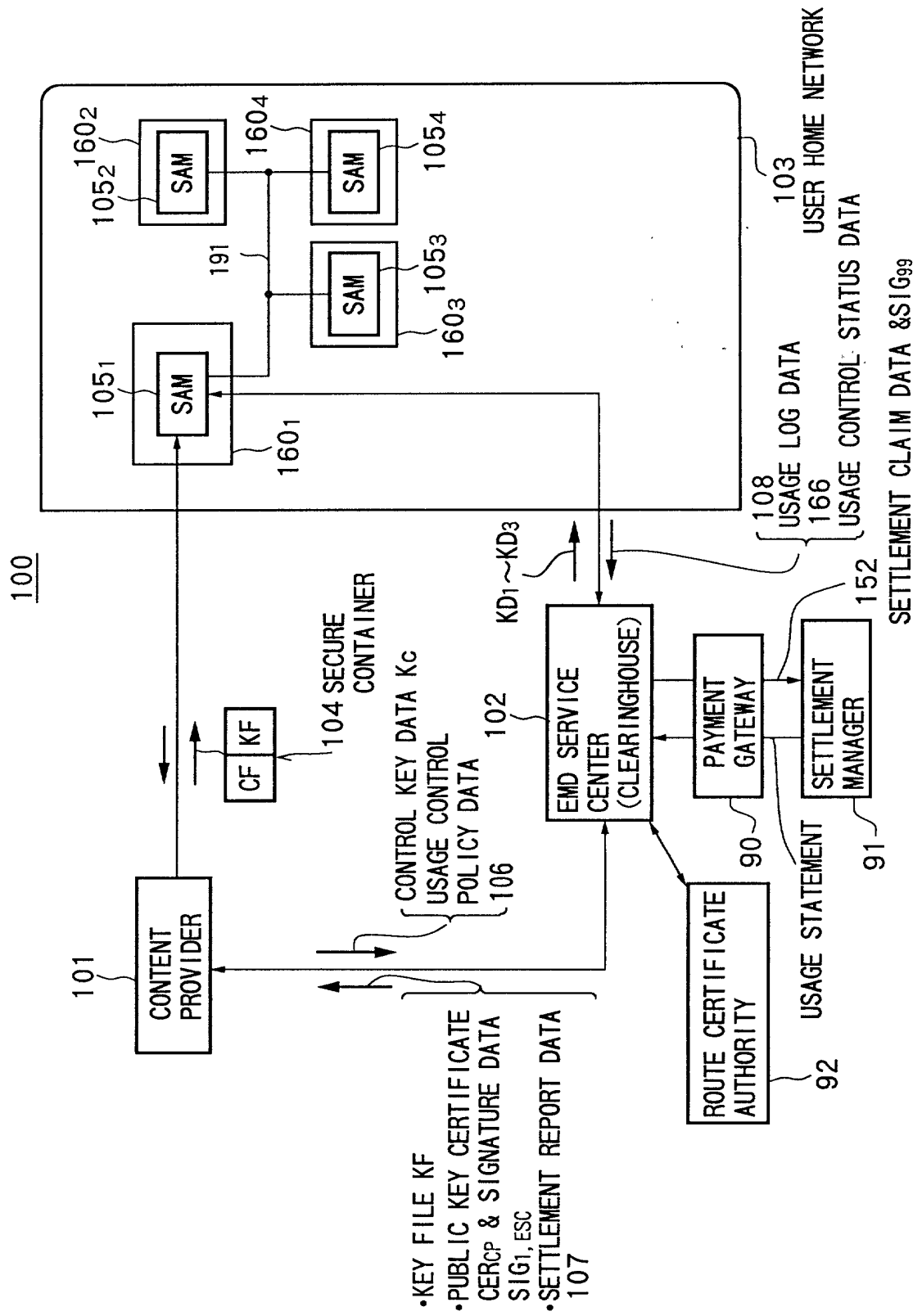




FIG.2

CONCEPT OF SECURE CONTAINER OF PRESENT INVENTION

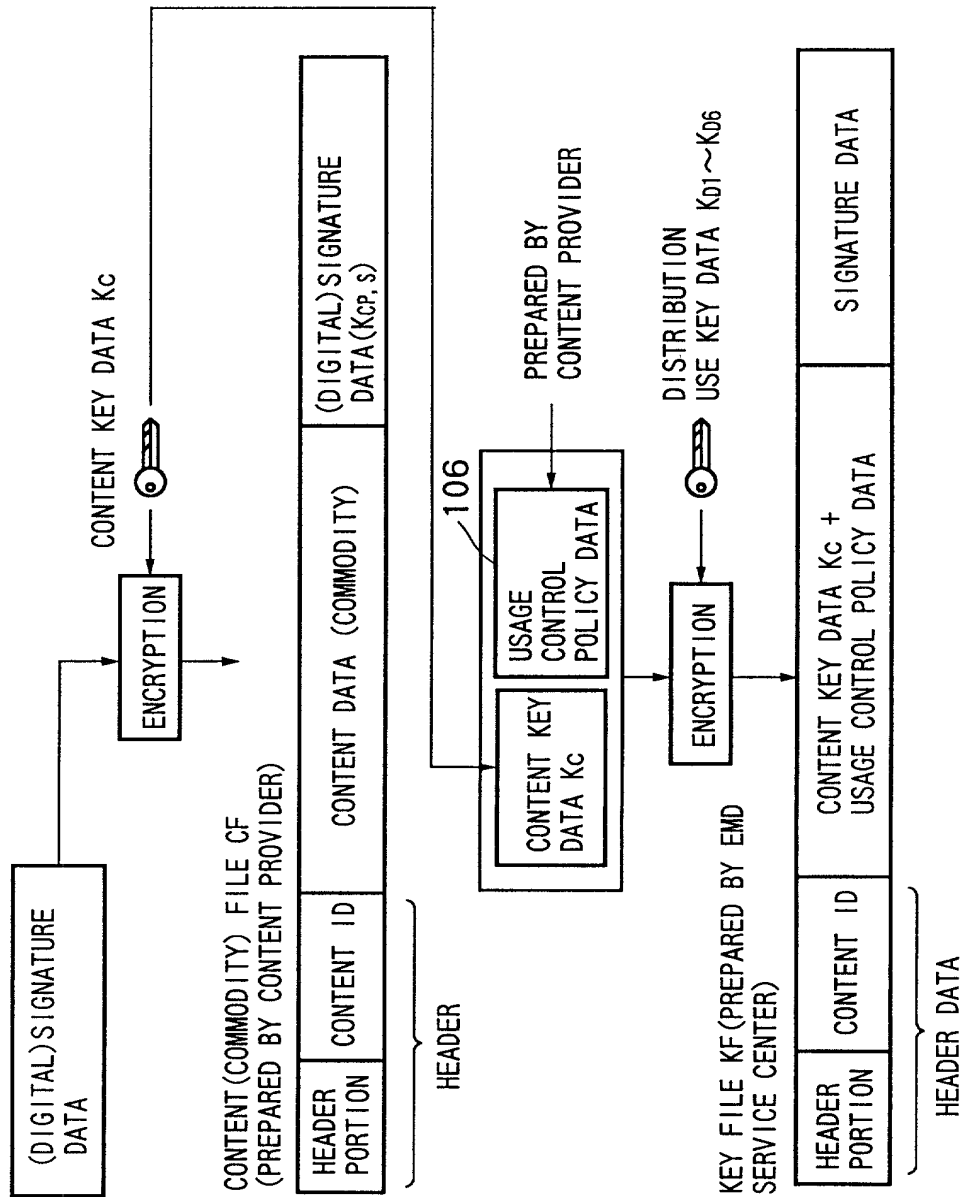


FIG. 3

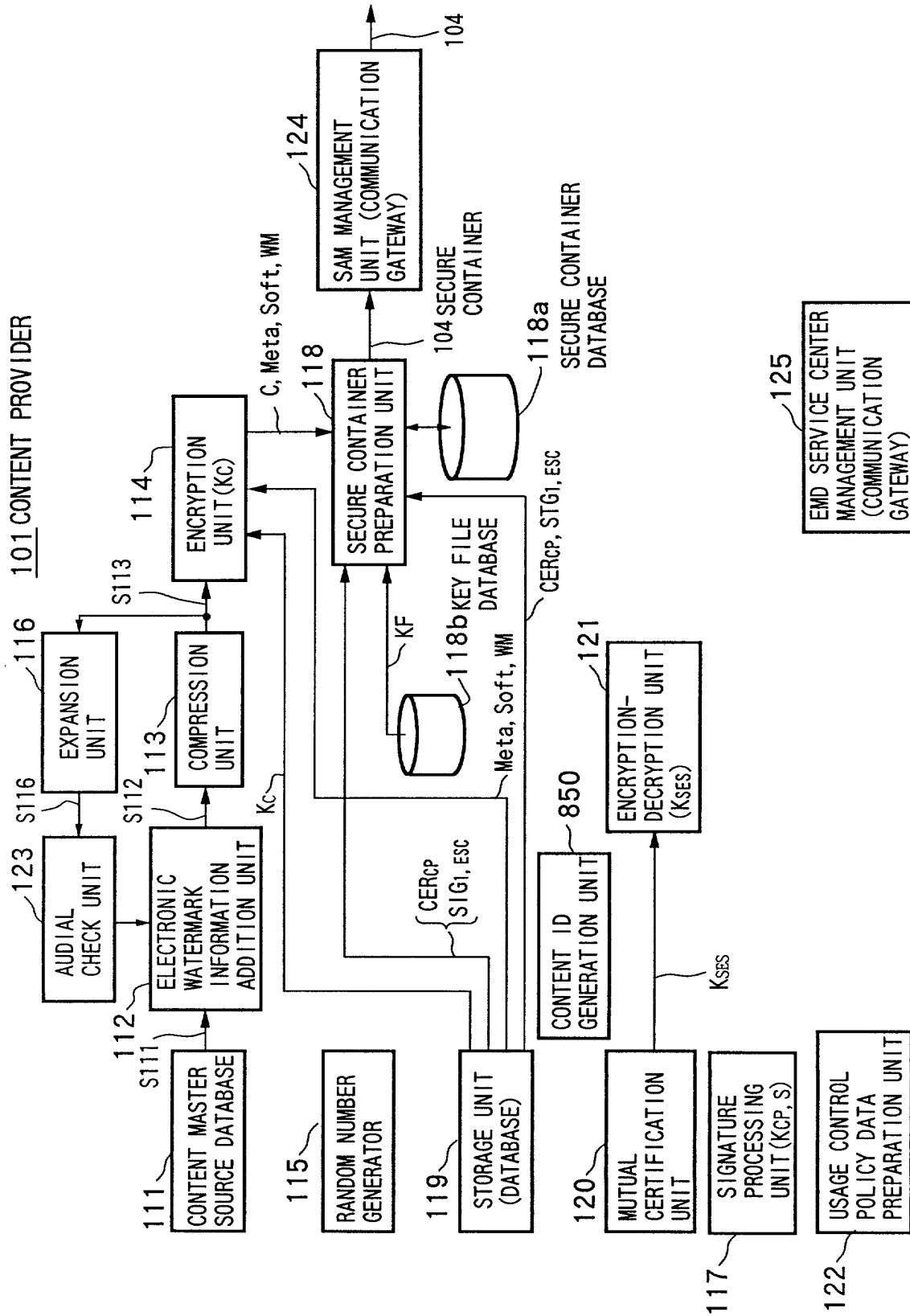
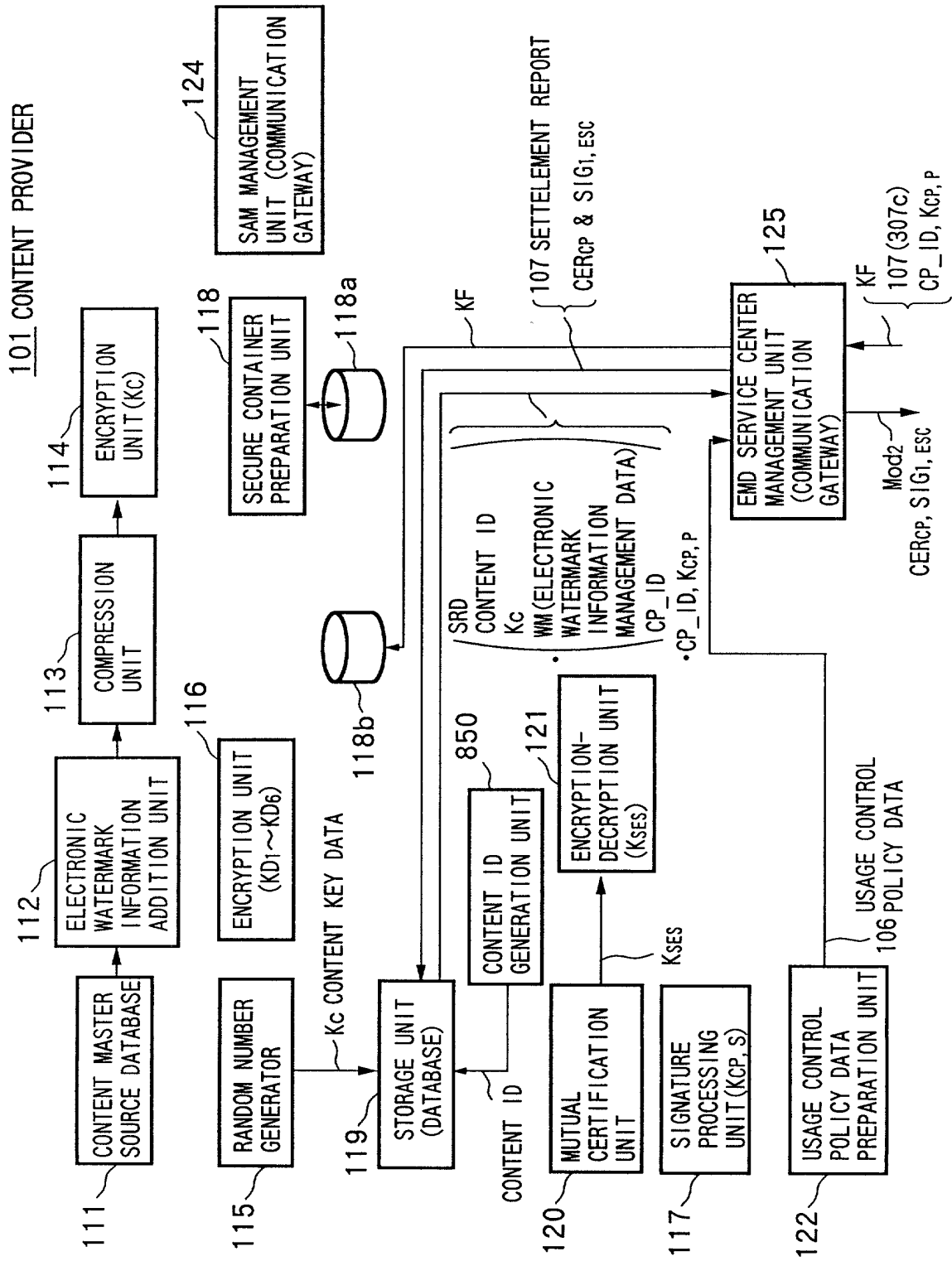


FIG. 4



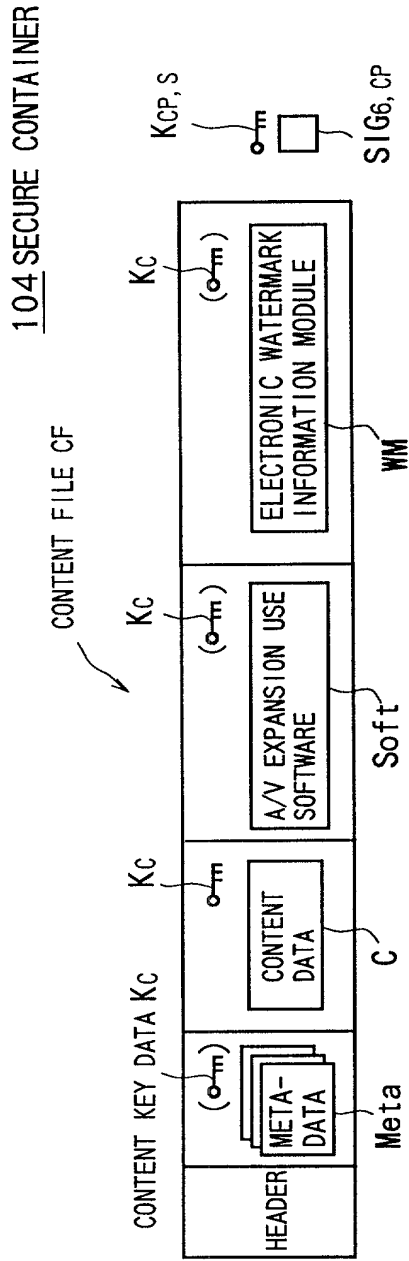


FIG. 5A

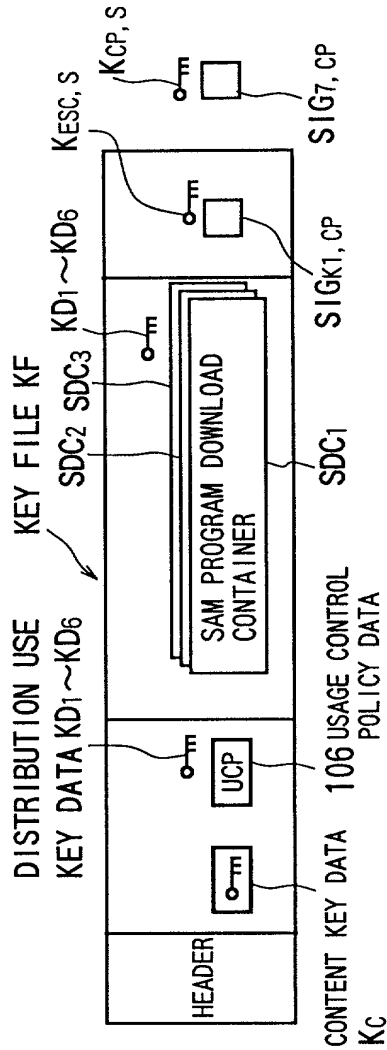


FIG. 5B

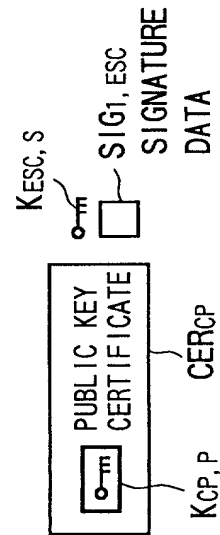


FIG. 5C

FIG.6

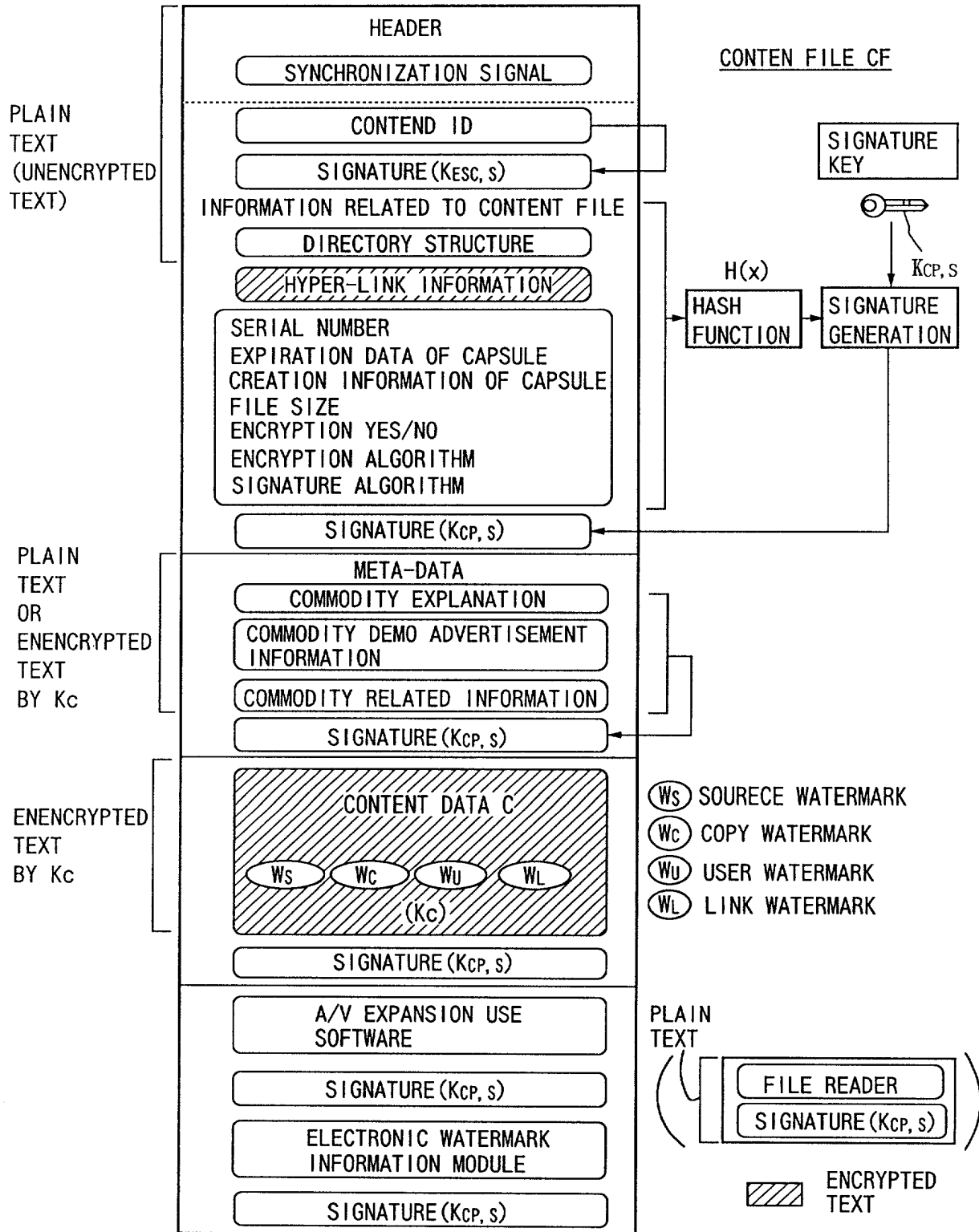


FIG. 7

KEY FILE CF

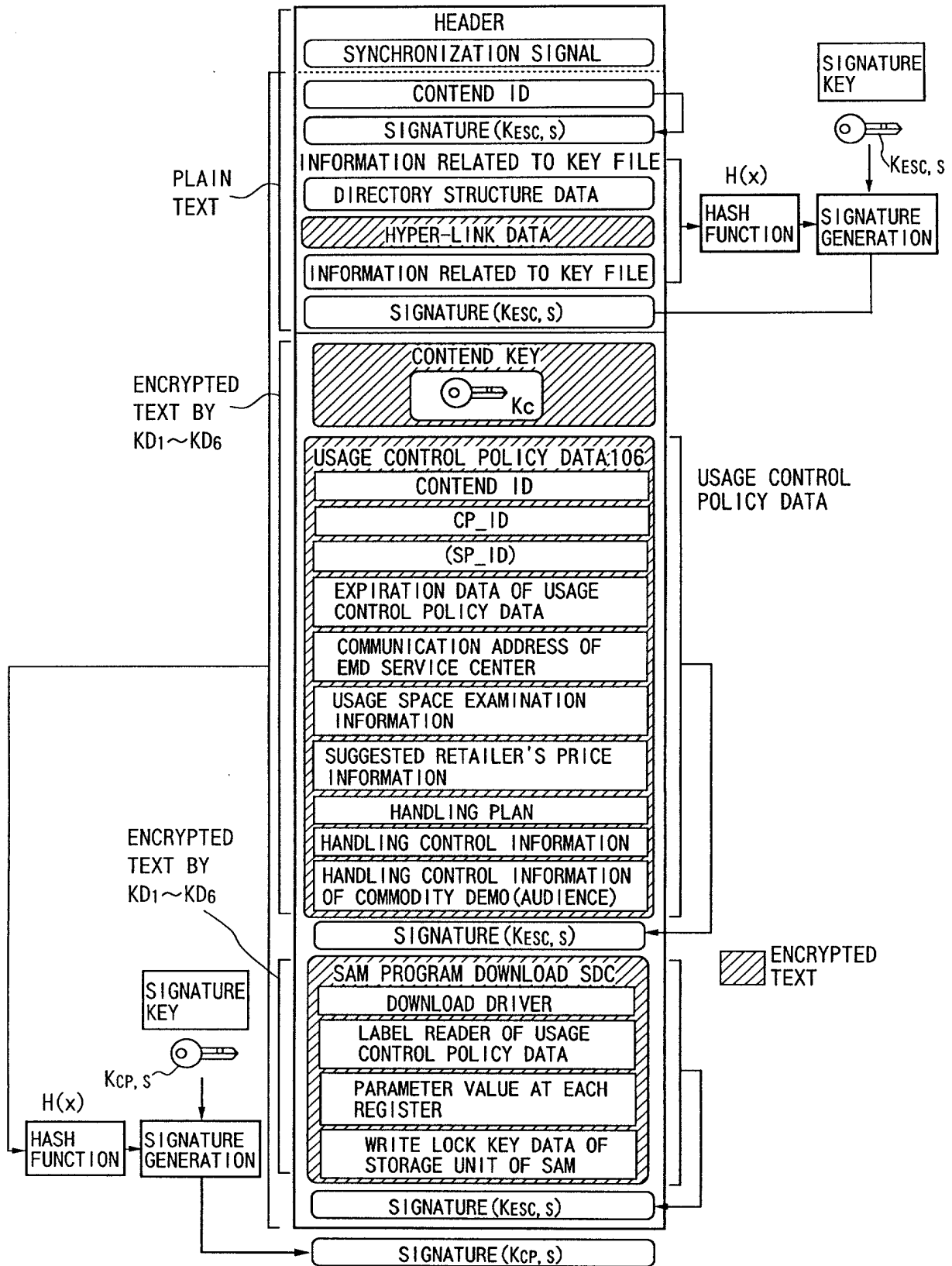


FIG.8

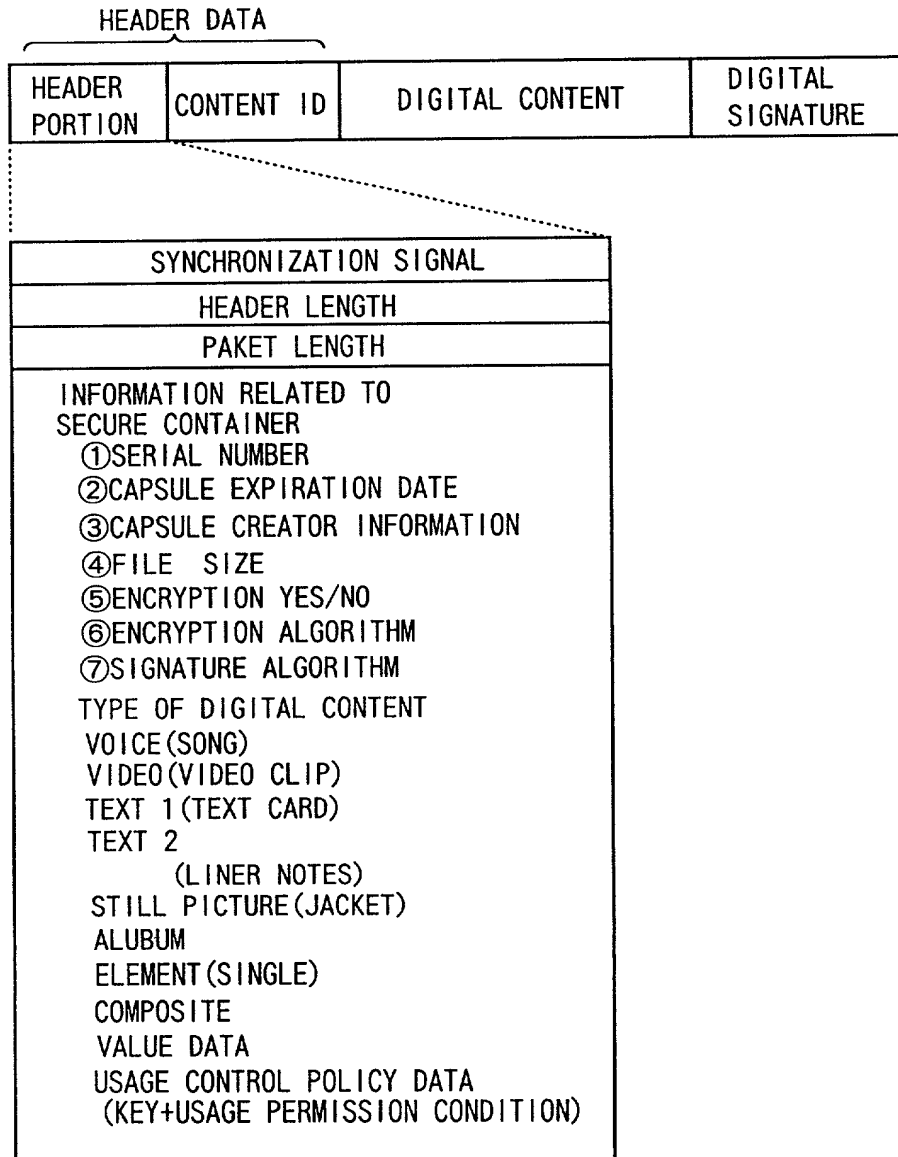


FIG.9

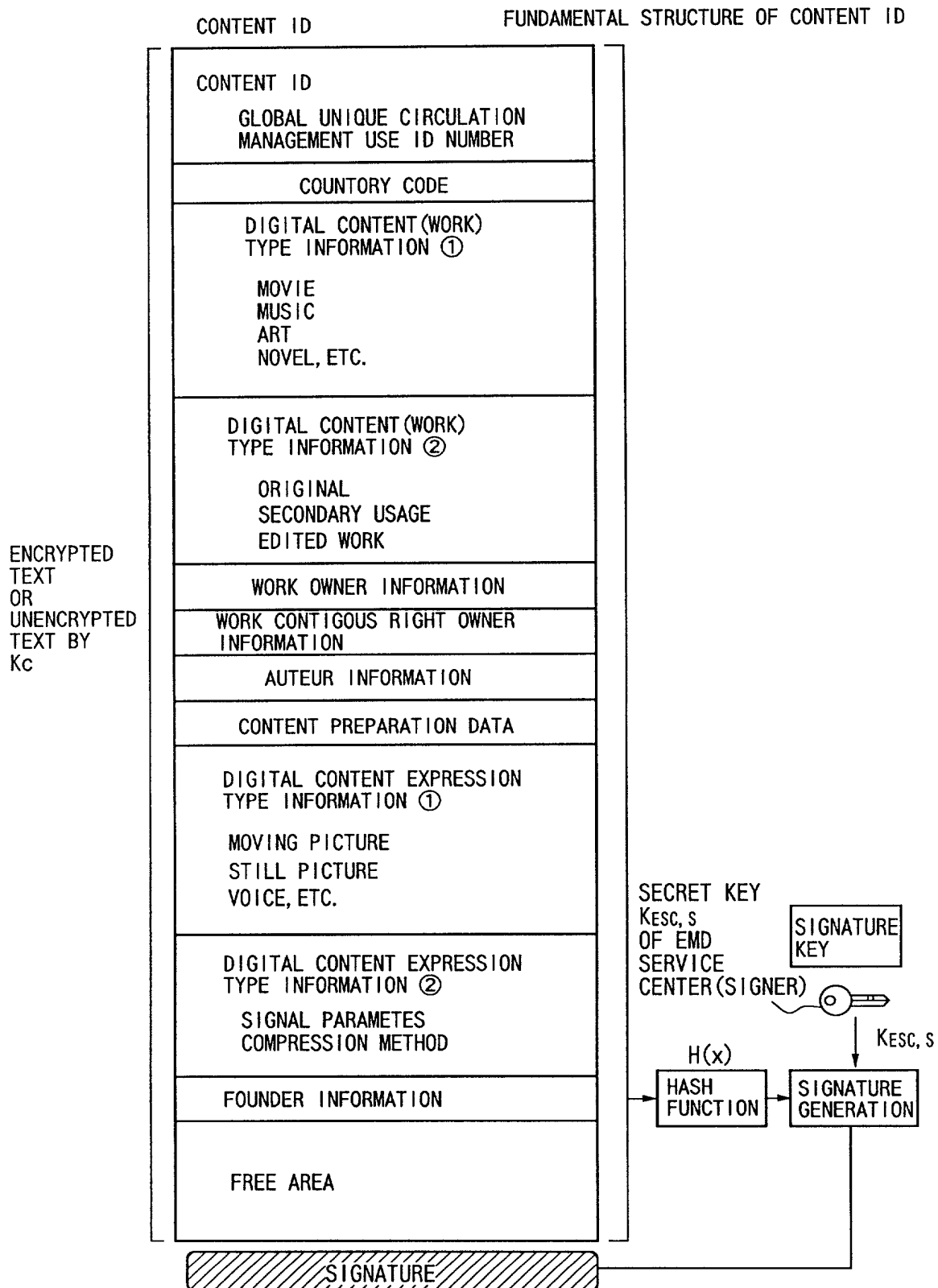




FIG.10

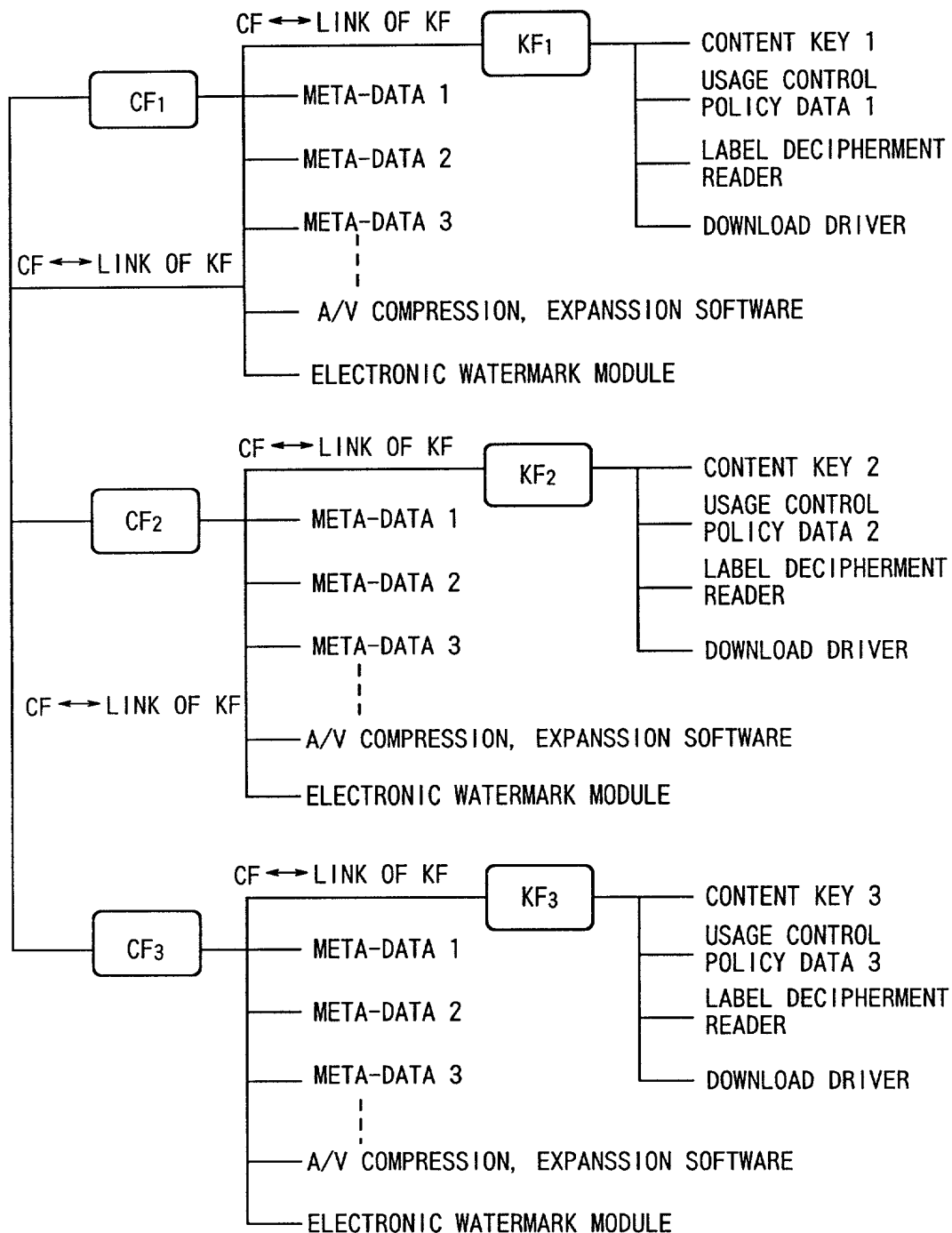
DIRECTORY STRUCTURE OF SECURE CONTAINER

FIG.11

## HYPER-LINK DATA OF SECURE CONTAINER

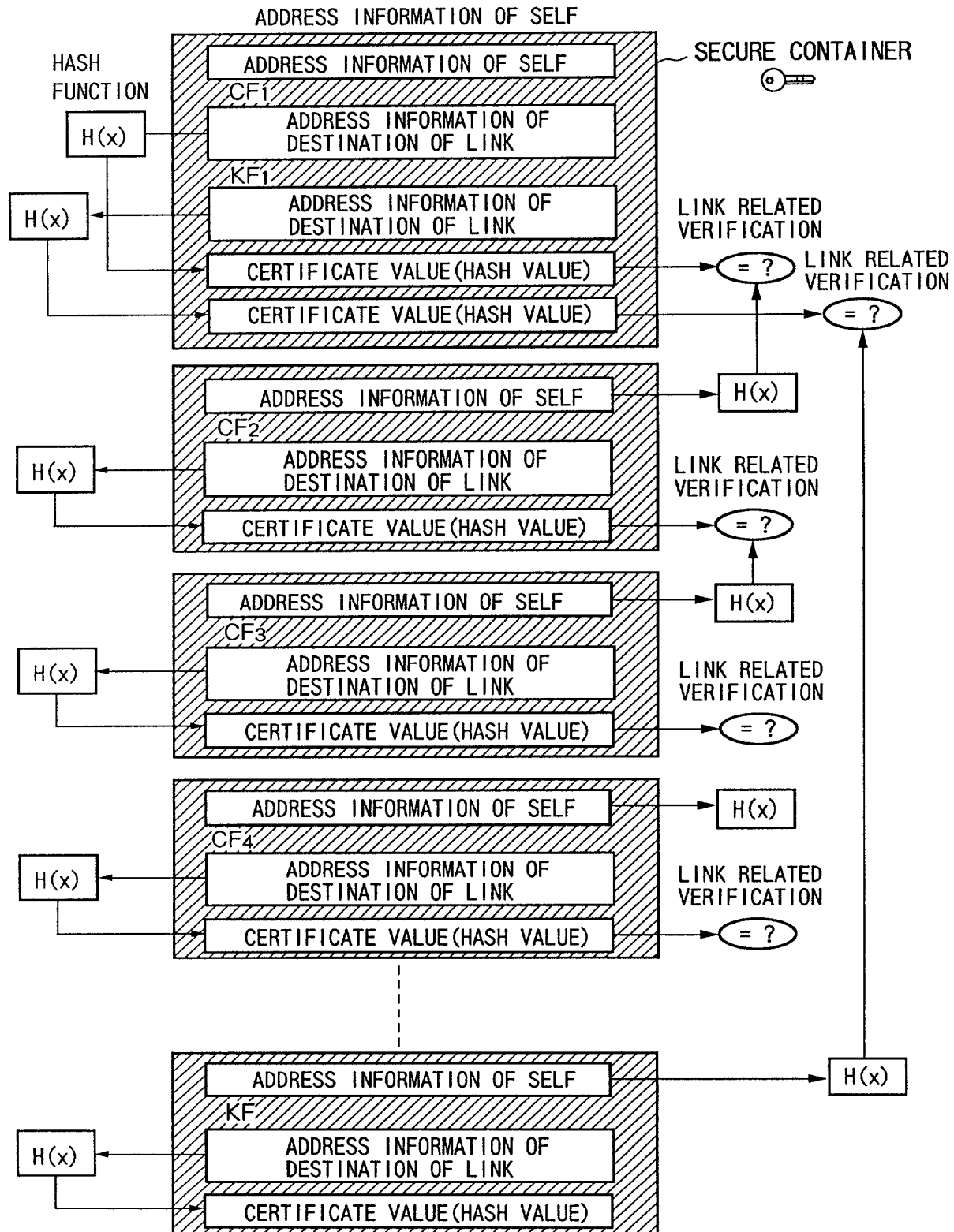


FIG.12

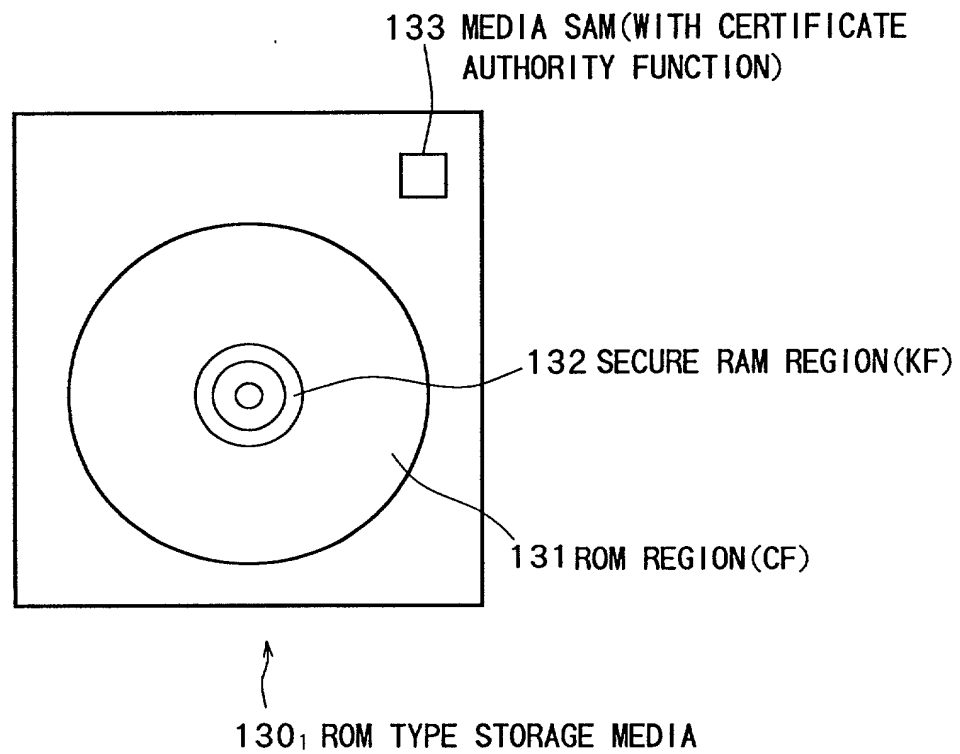


FIG.13

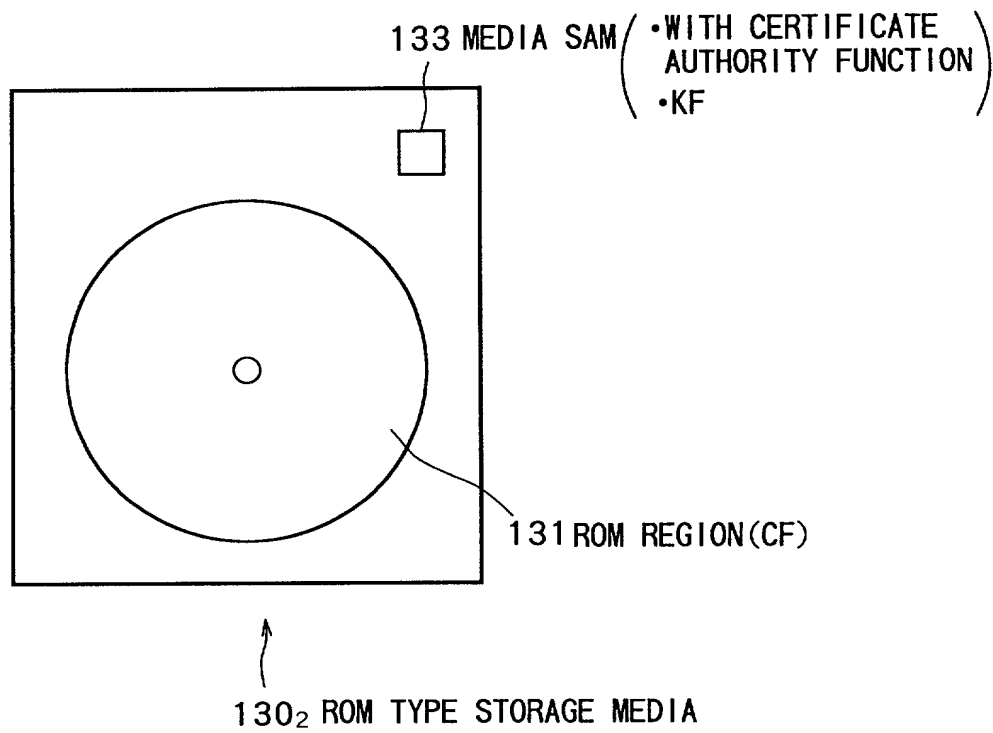


FIG.14

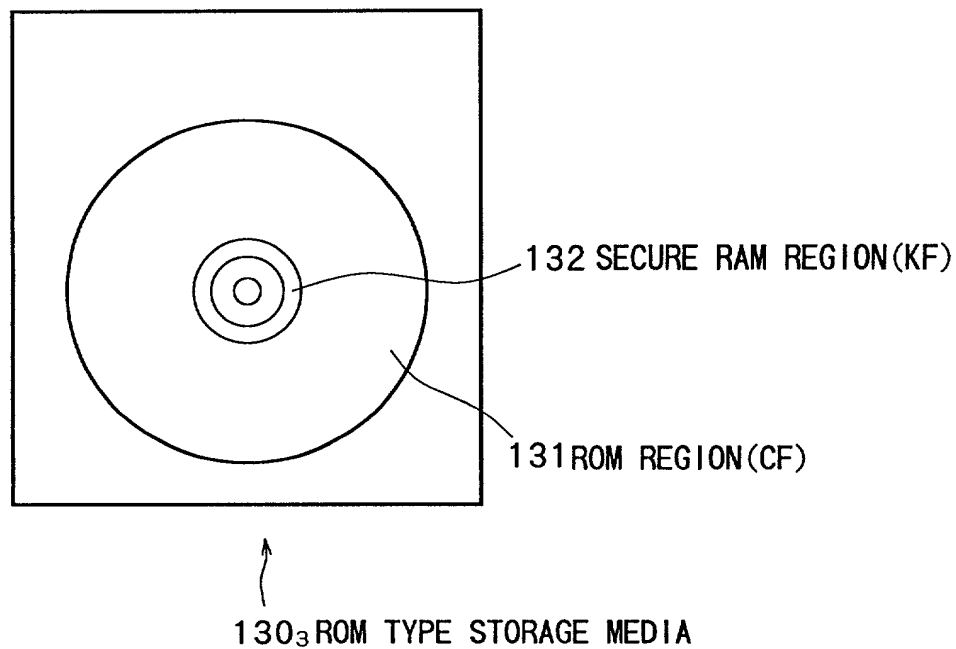


FIG.15

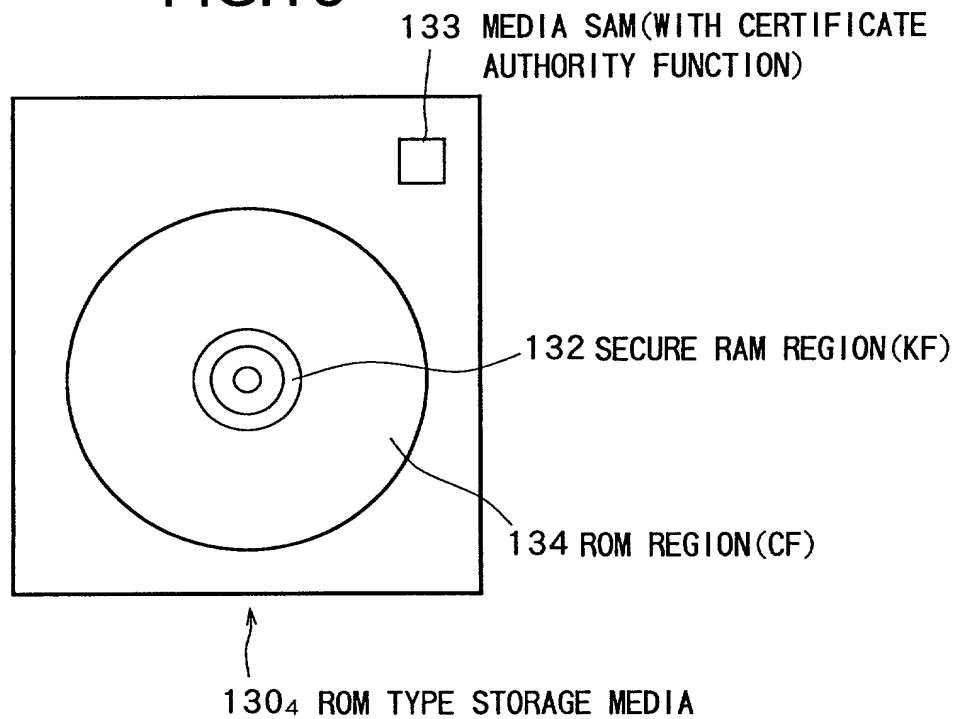


FIG.16

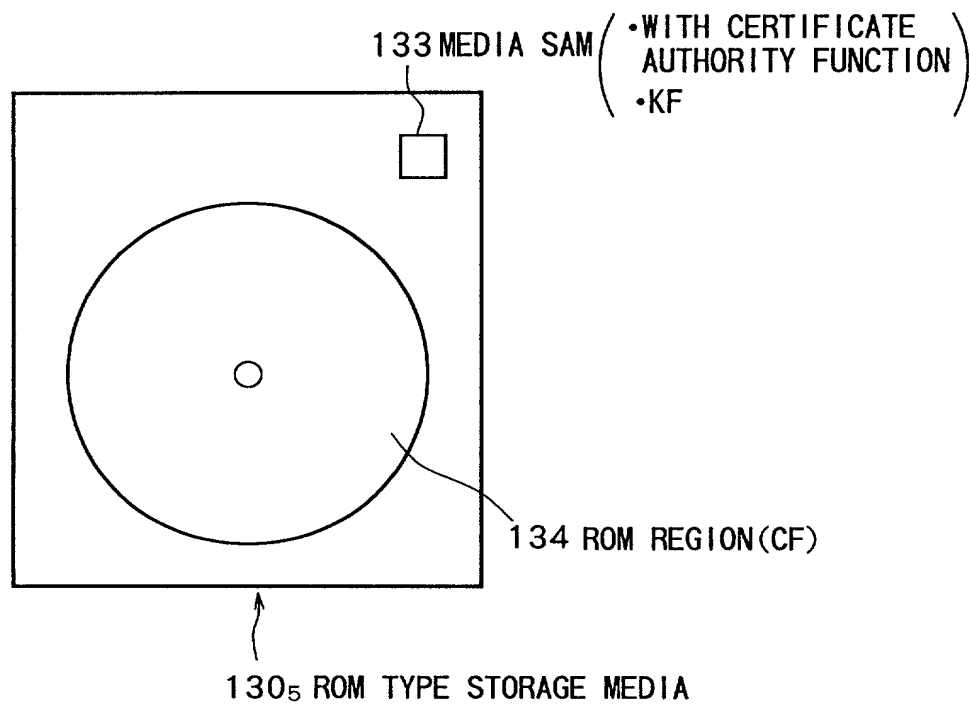


FIG.17

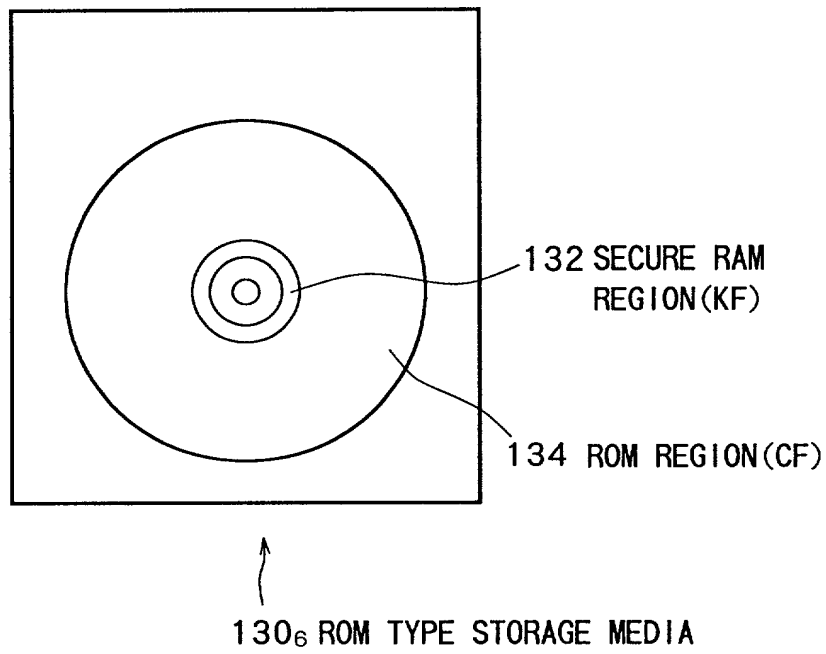


FIG.18

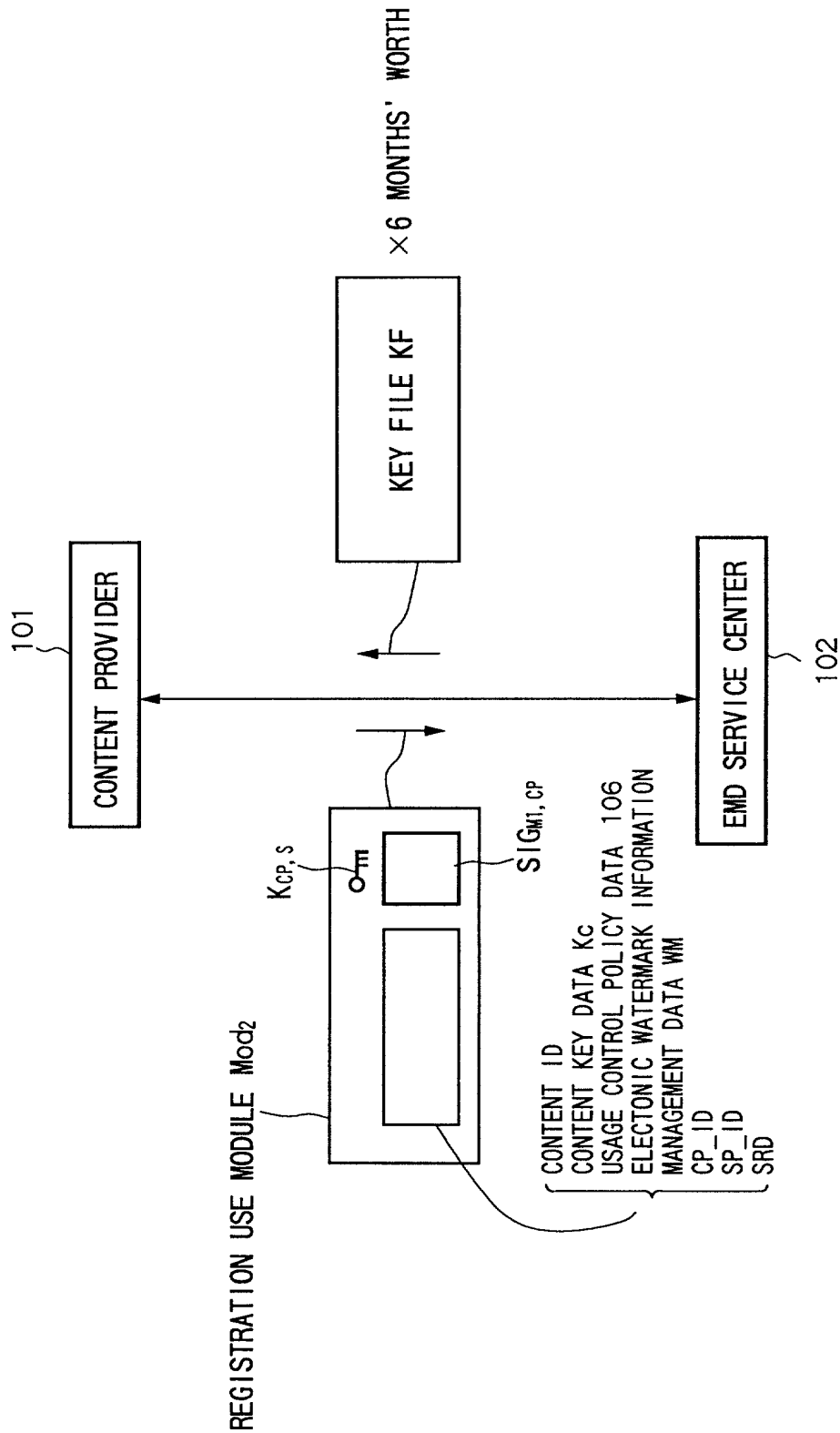


FIG.19

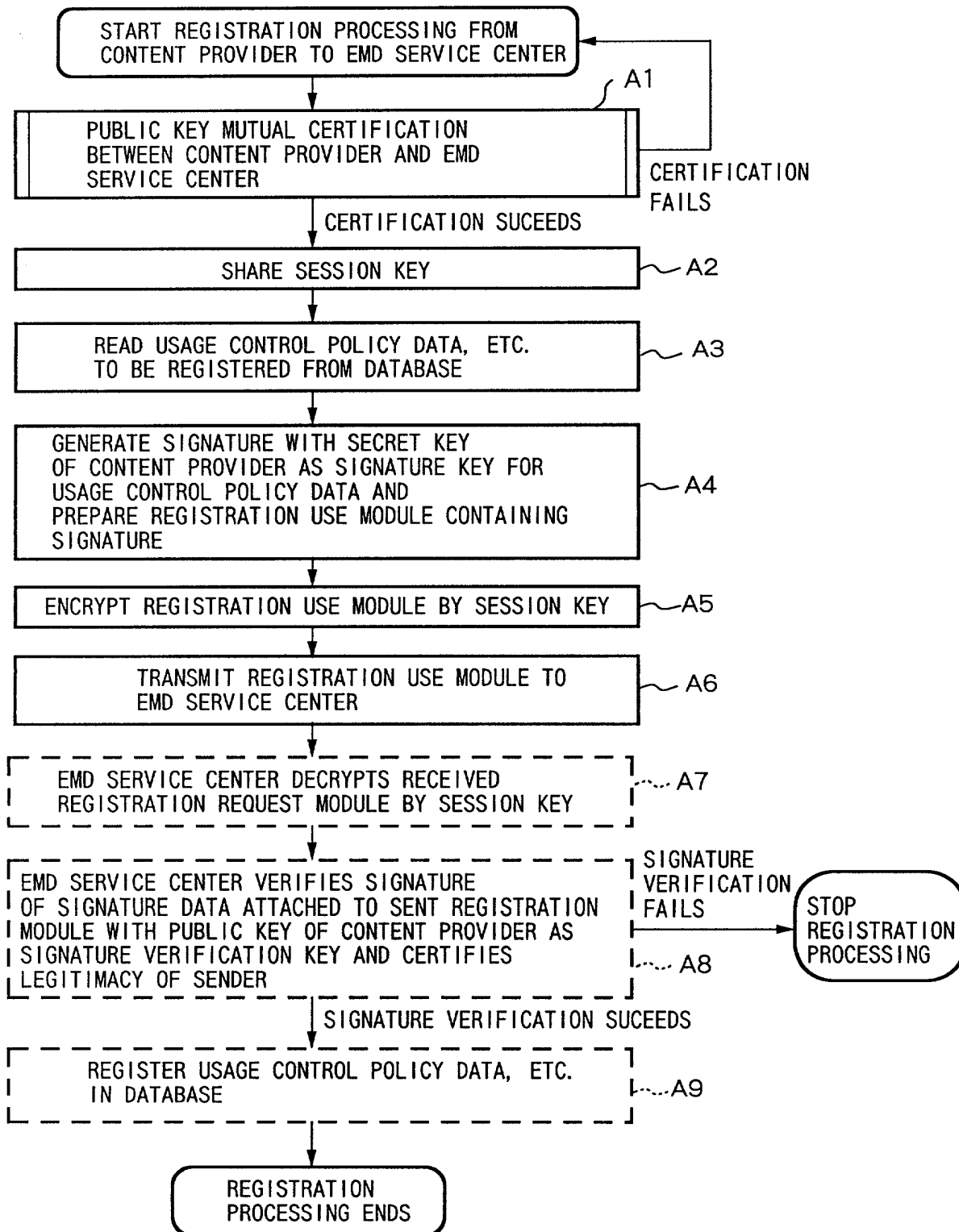




FIG.20

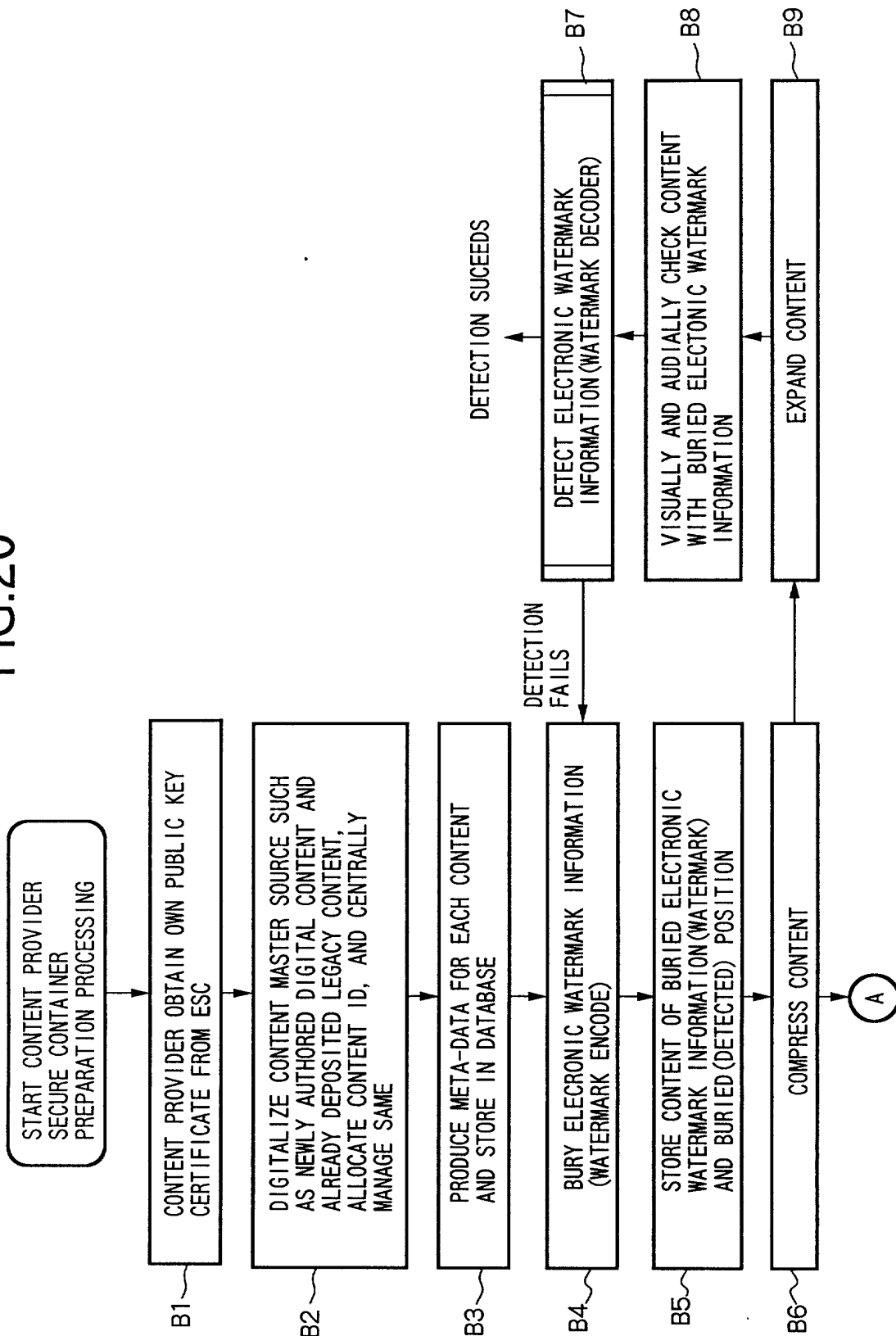


FIG.21

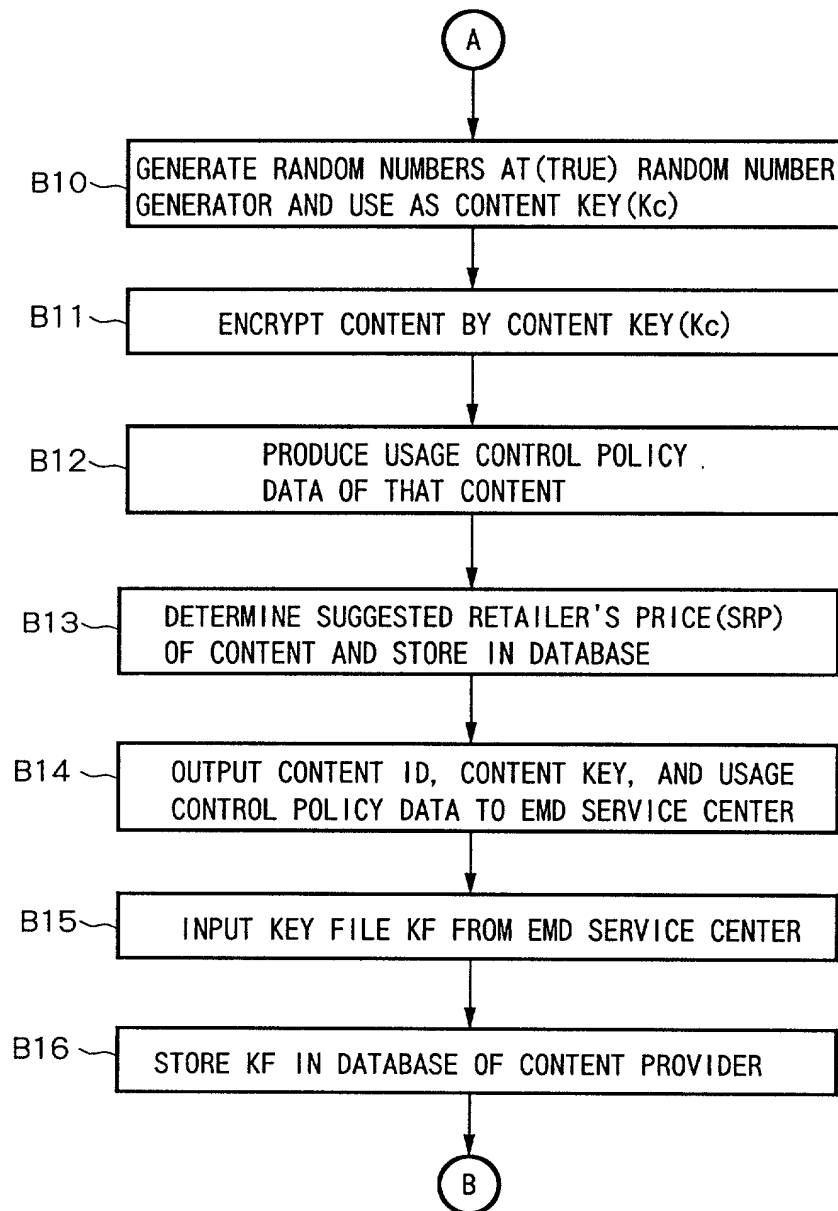
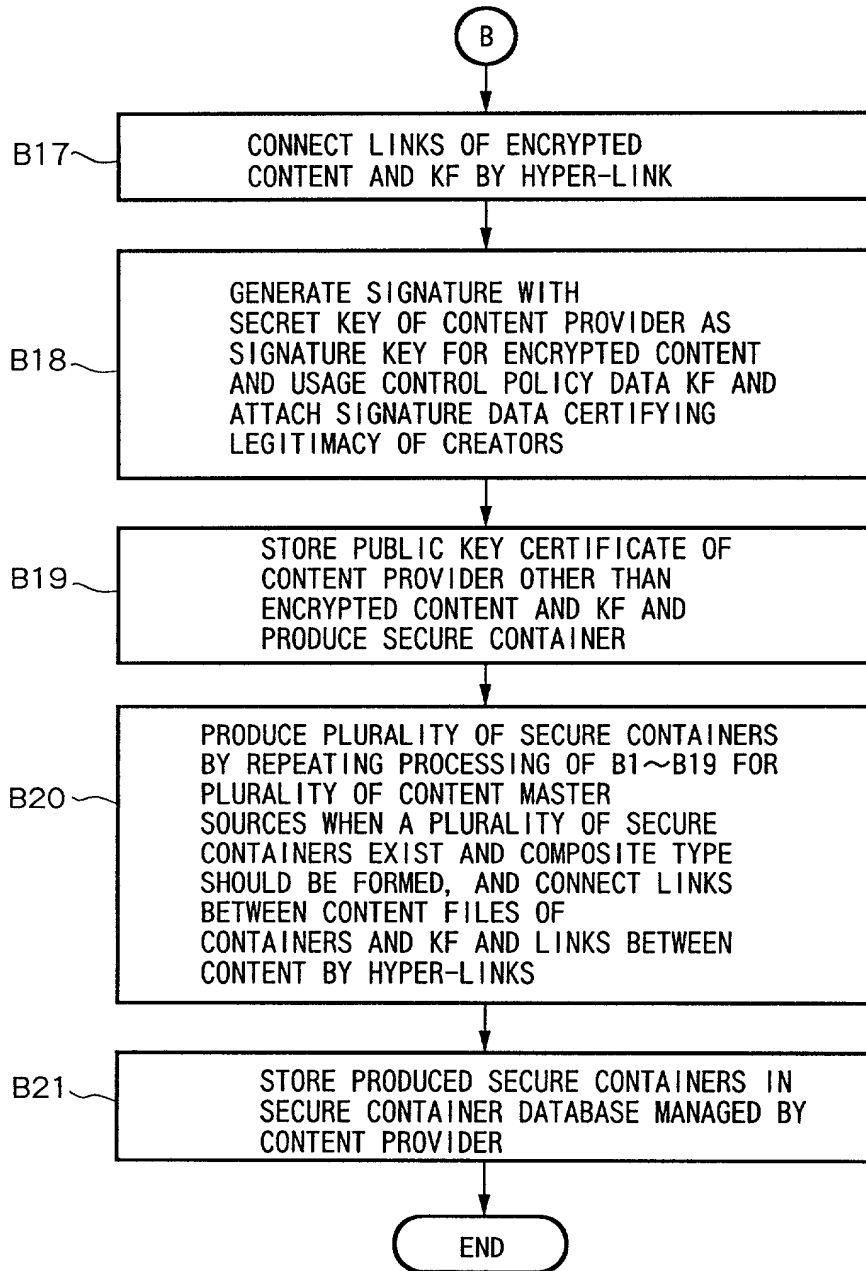
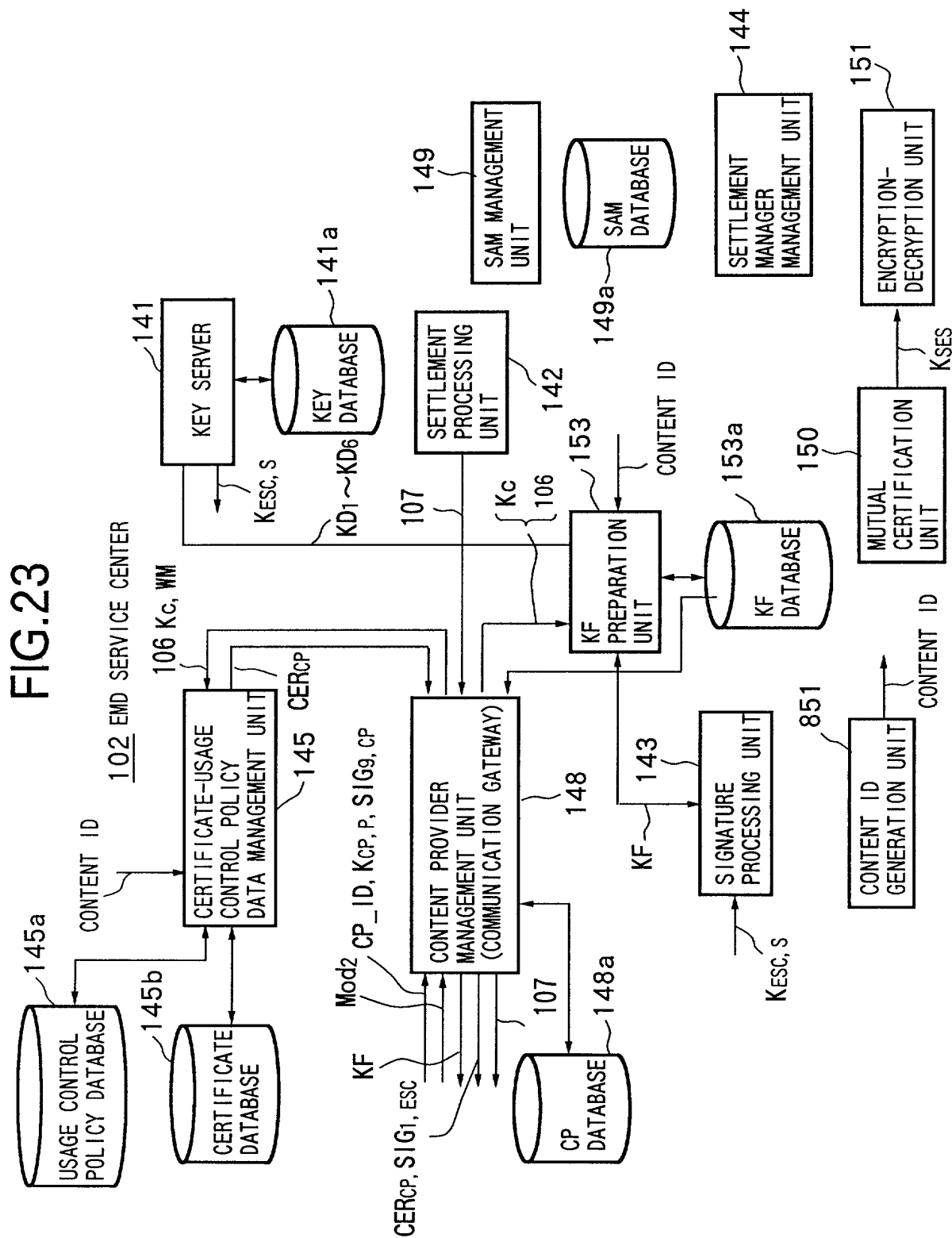


FIG.22





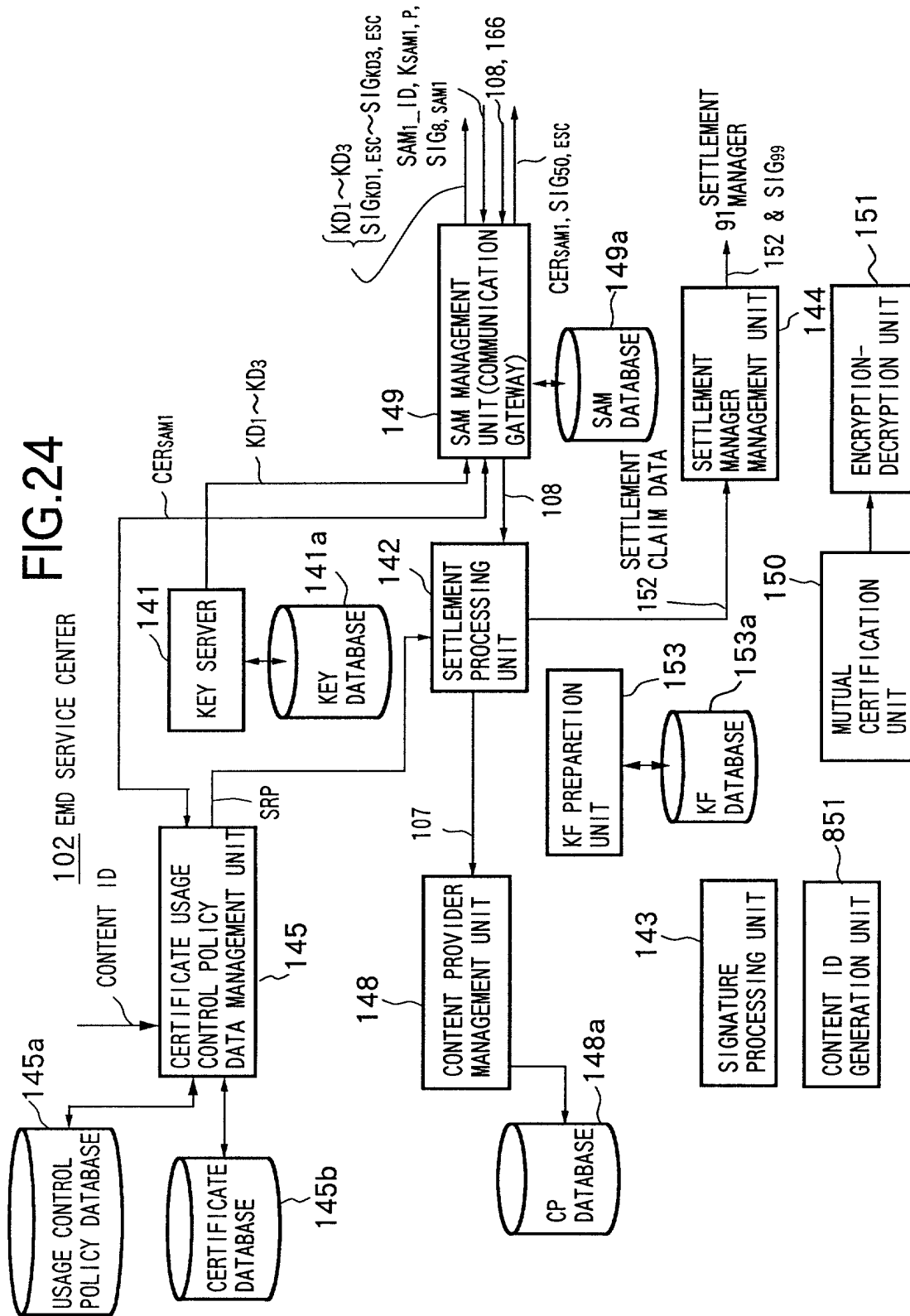


FIG.25

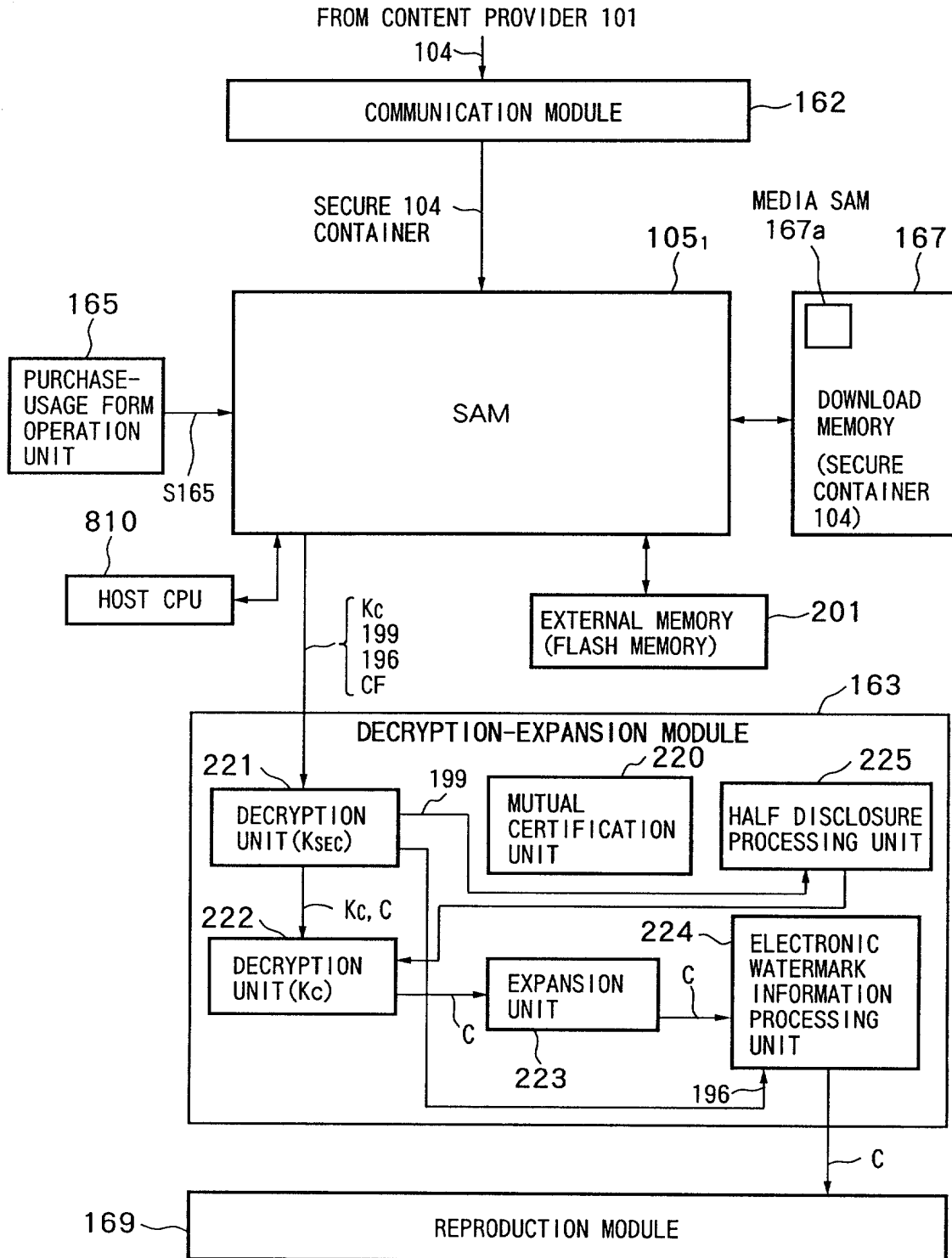
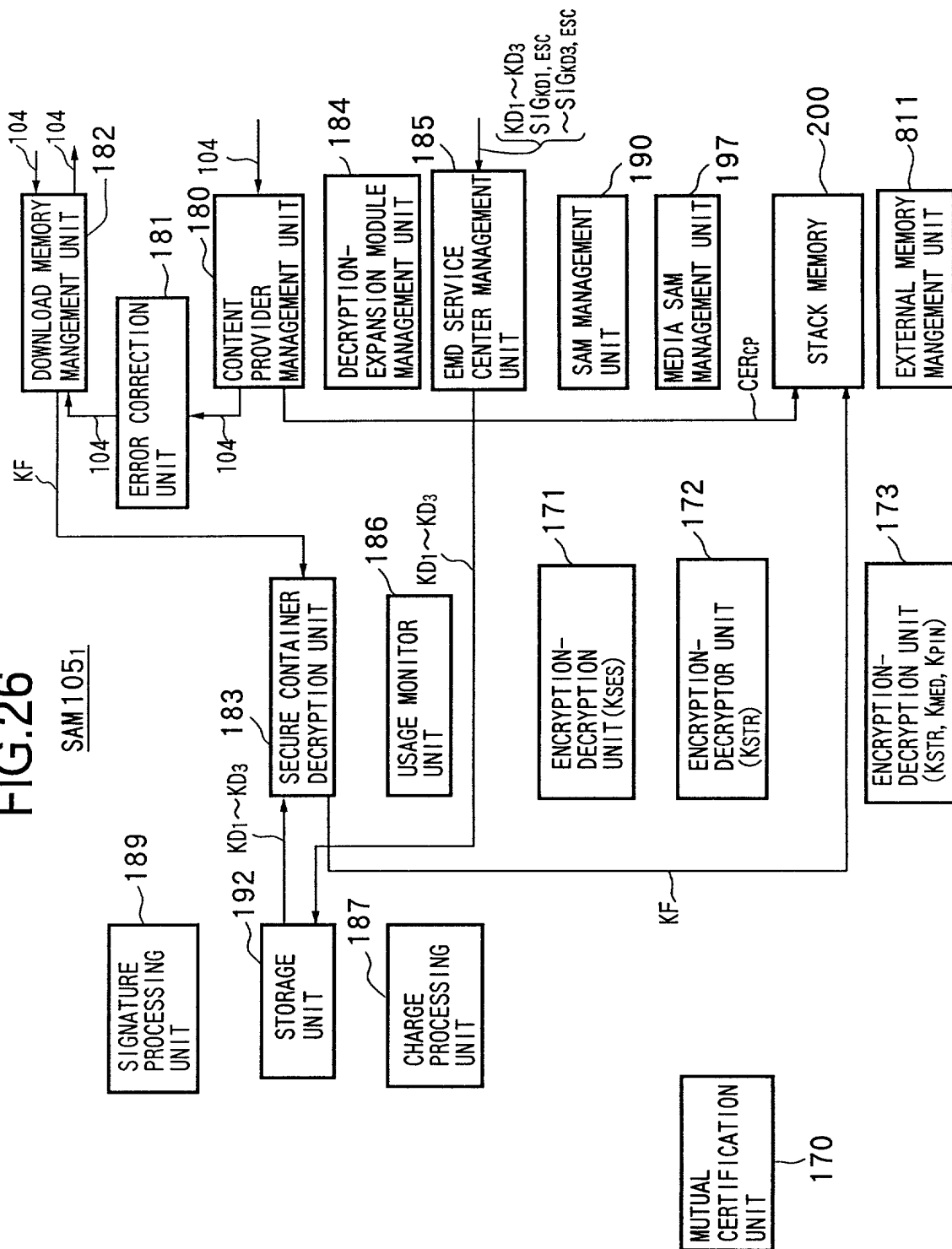


FIG. 26

SAM 105<sub>1</sub>

## FIG.27

DATA STORED IN EXTERNAL MEMORY 201

USAGE LOG DATA 108

SAM REGISTRATION LIST

## FIG.28

DATA STORED IN STACK MEMORY 200

CONTENT KEY DATA  $K_c$

USAGE CONTROL POLICY DATA(USP) 106

LOCK KEY DATA  $K_{Log}$  OF STORAGE UNIT(FLASH MEMORY) 192

CERTIFICATE  $CER_{CP}$  OF CONTENT PROVIDER 101

USAGE CONTROL STATUS DATA(UCS) 166

SAM PROGRAM DOWNLORD CONTAINERS  $SD_1$  TO  $SD_3$



FIG.29

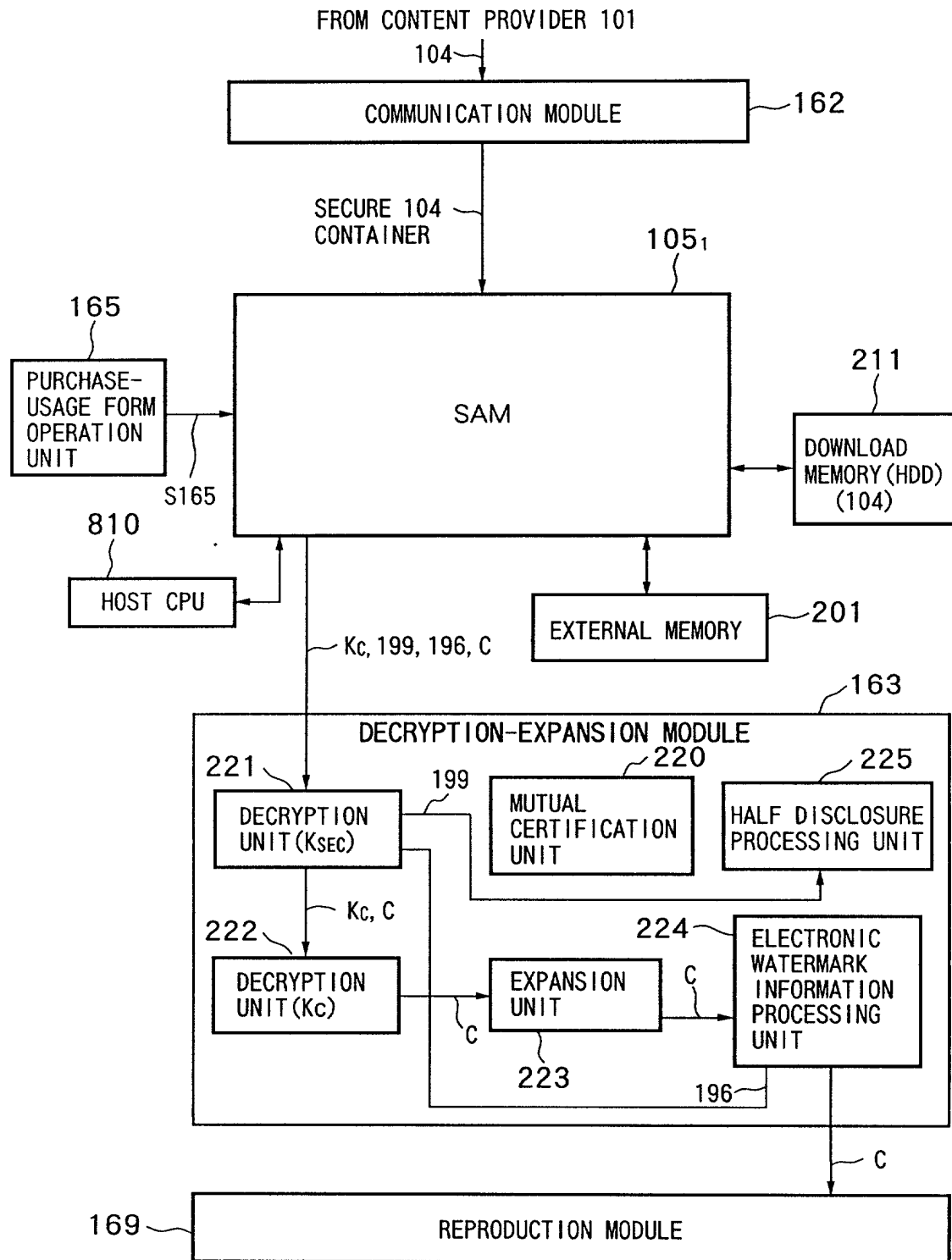
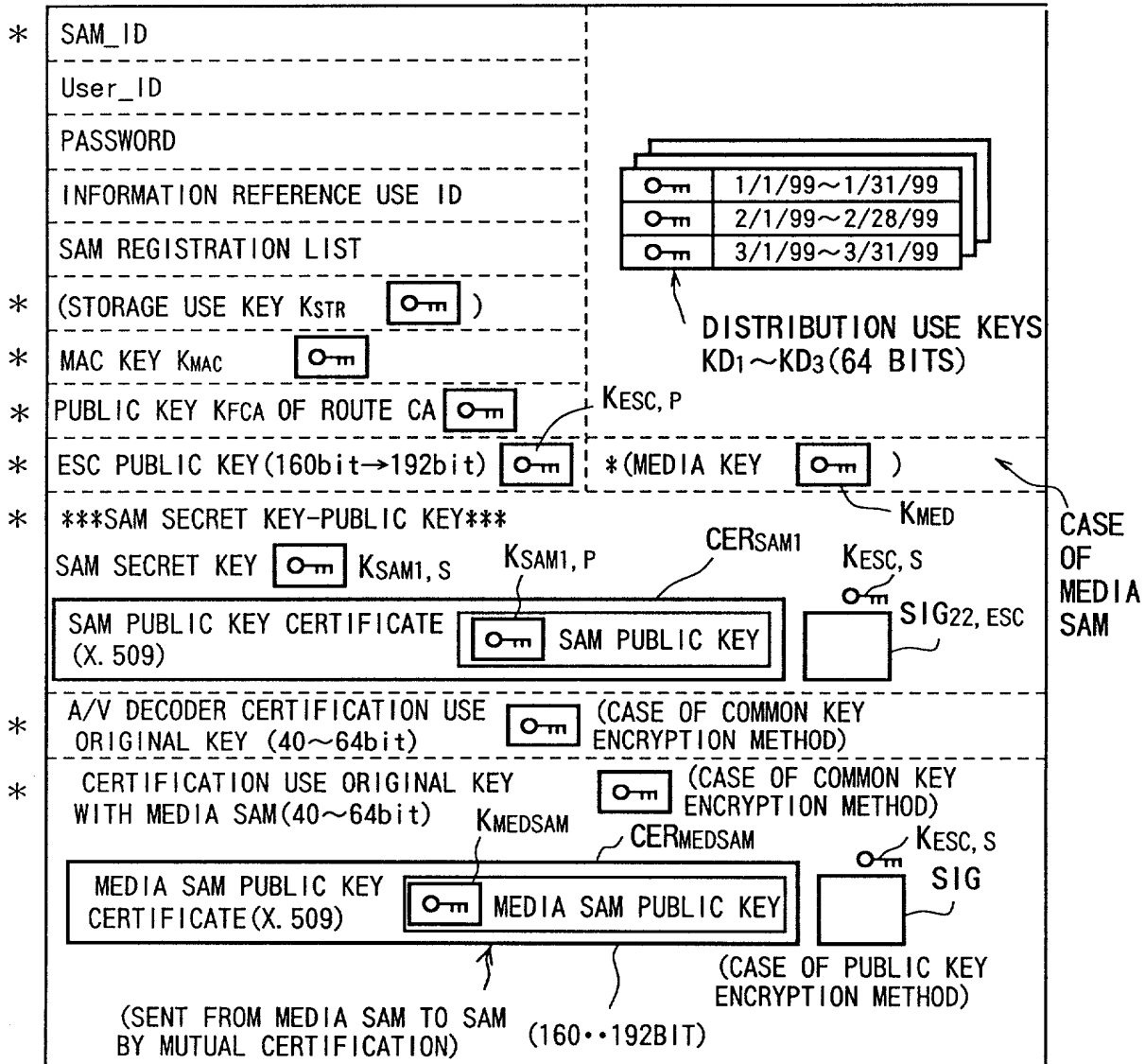
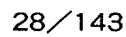


FIG.30

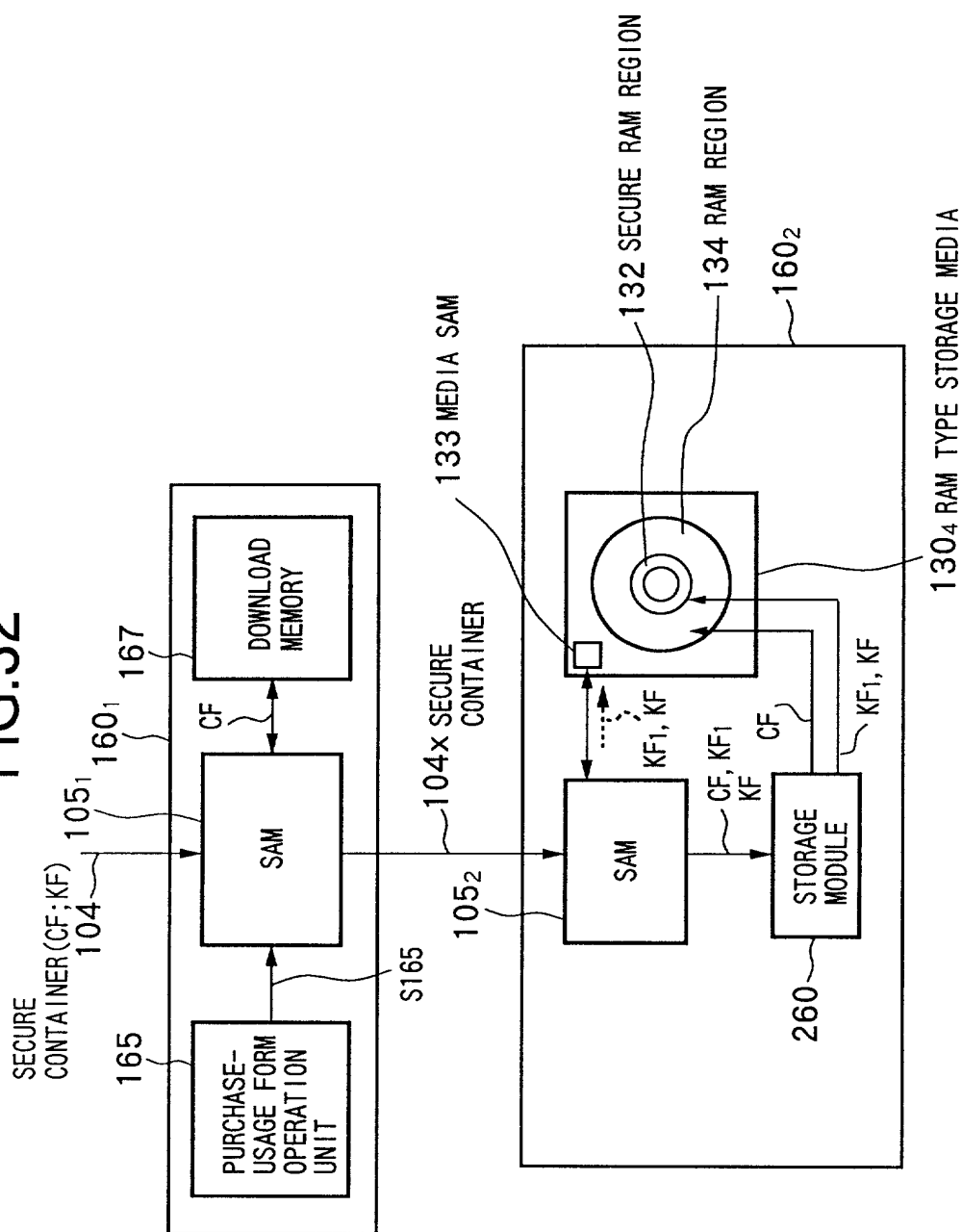
## DATA STORED IN STORAGE UNIT 192



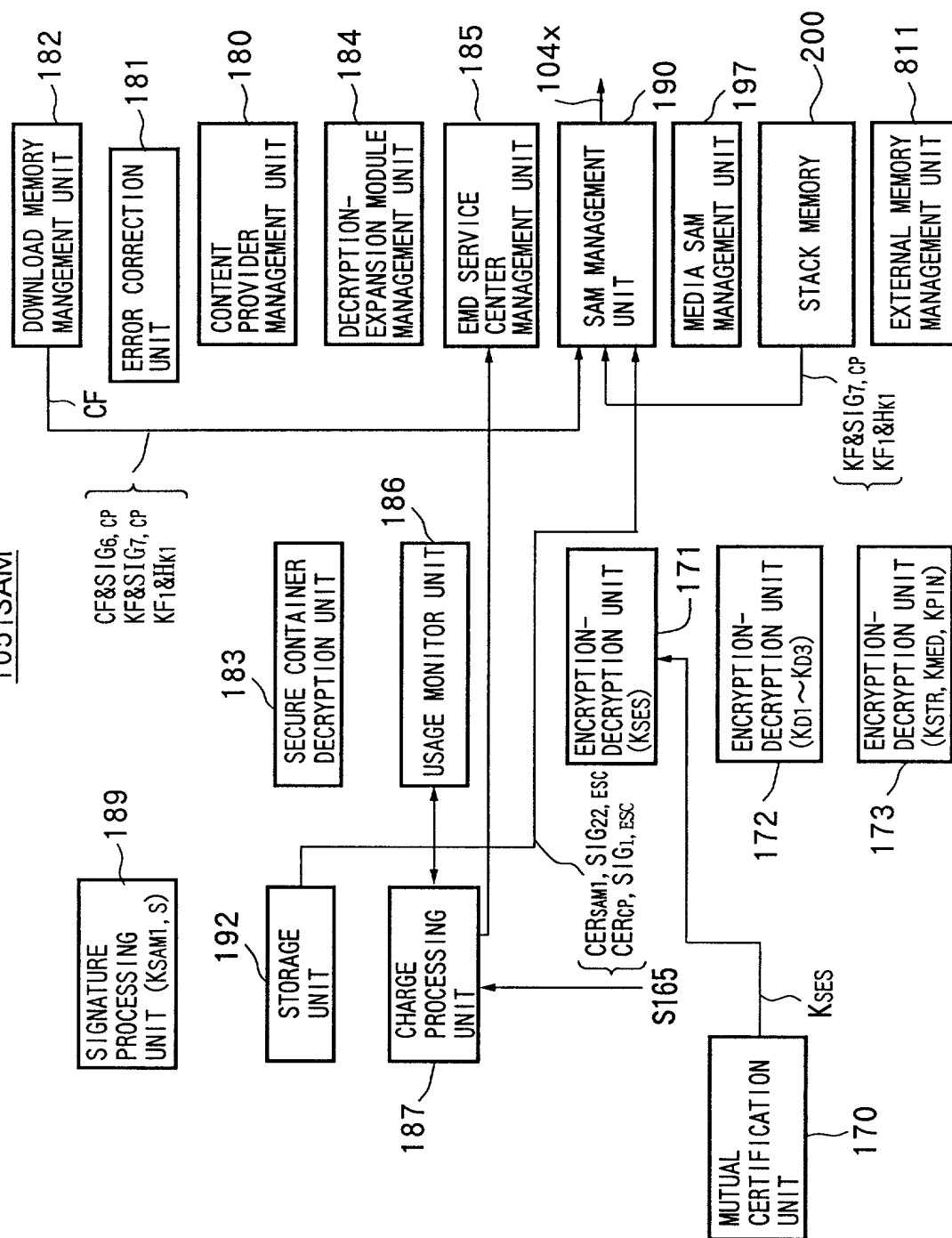
105<sub>1</sub>~105<sub>4</sub>SAM



29/143



1051SAM



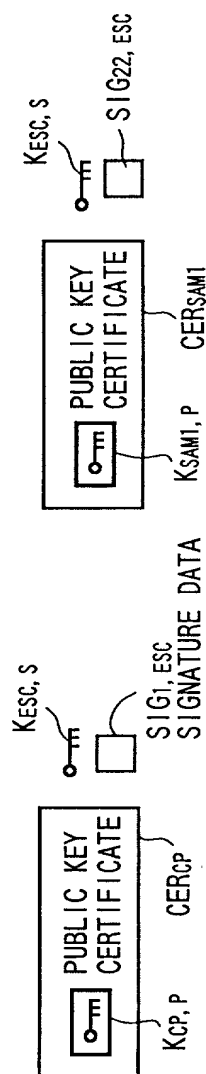
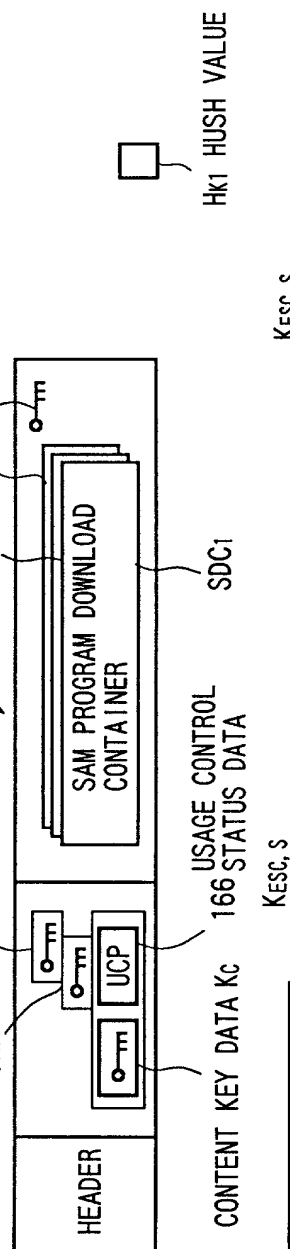
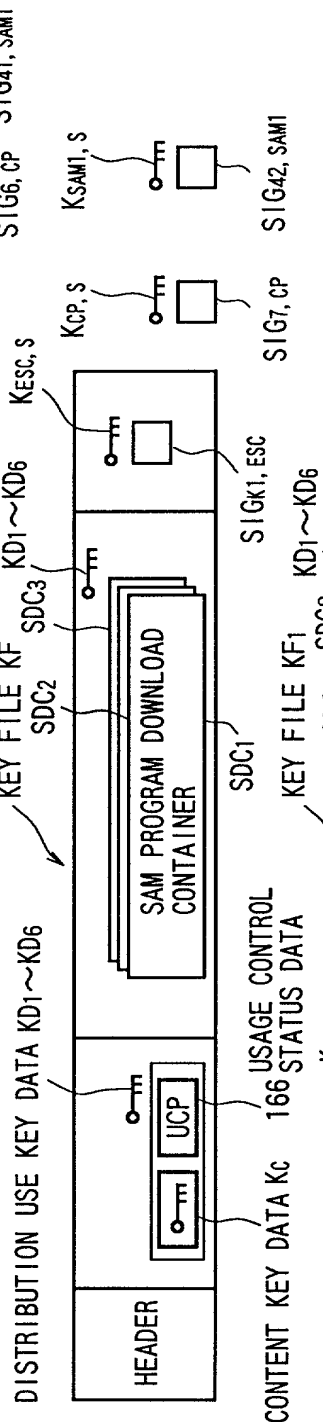
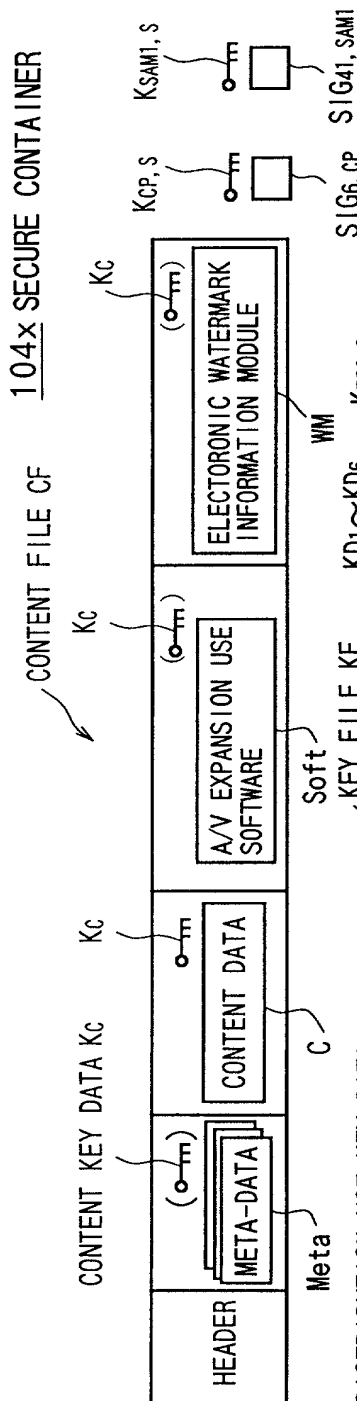


FIG. 35

SAM1052

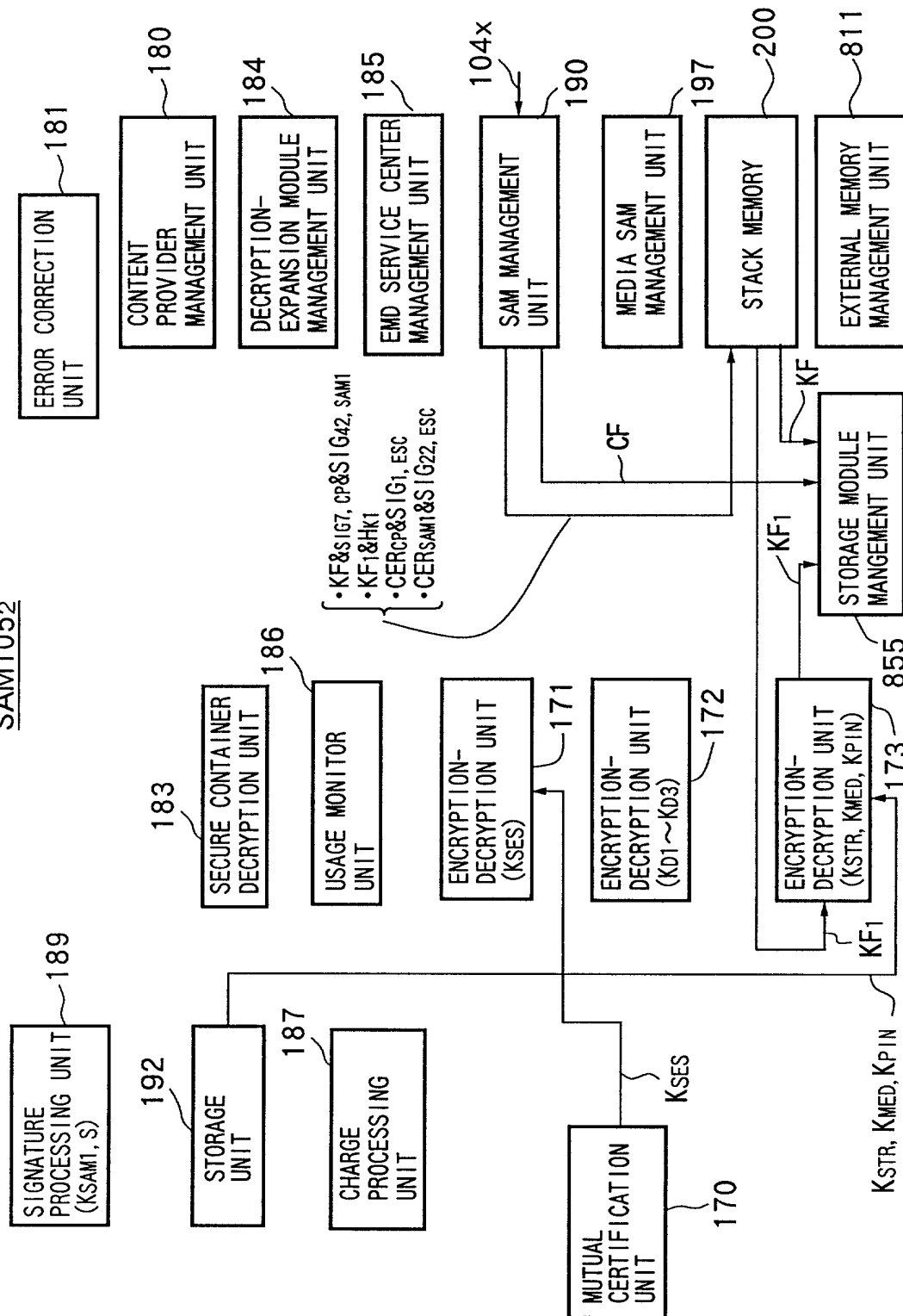


FIG.36

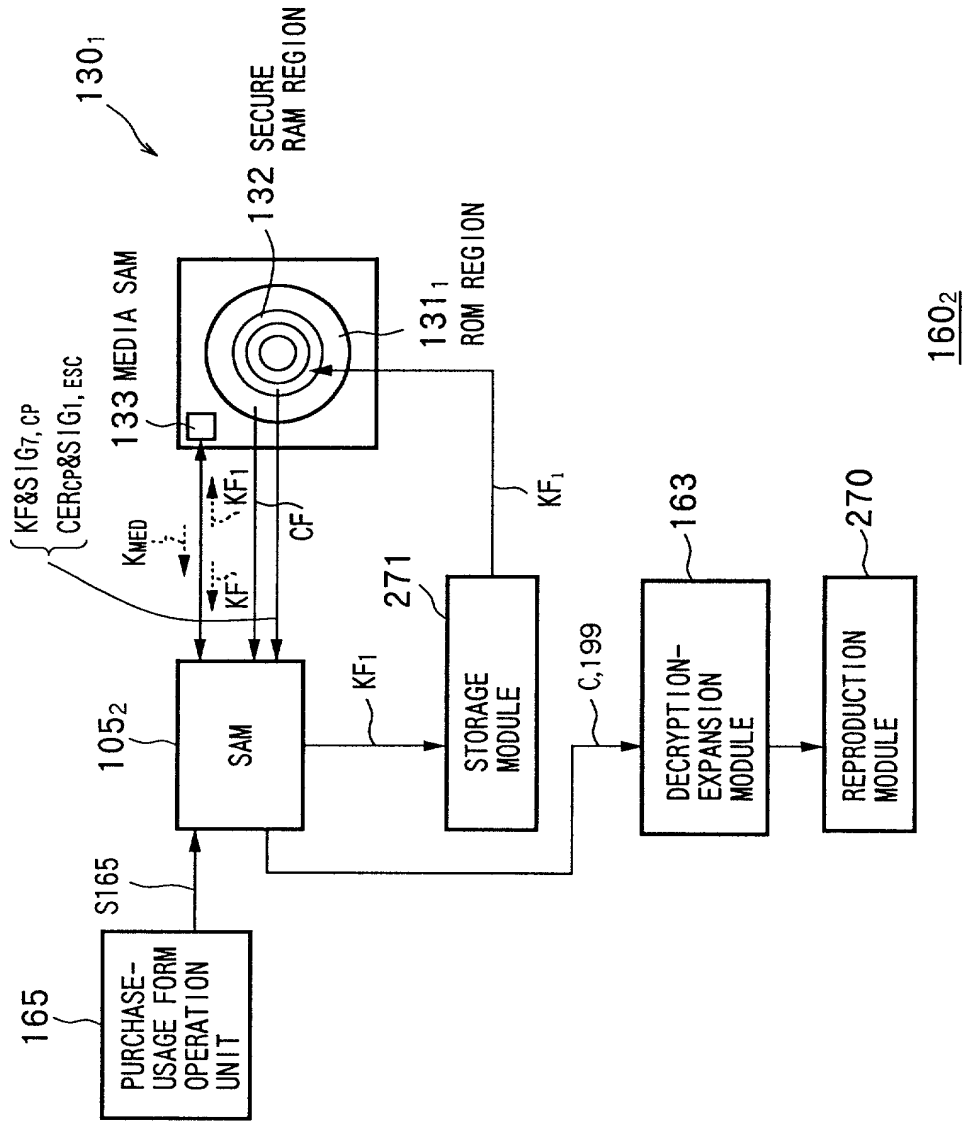




FIG. 37

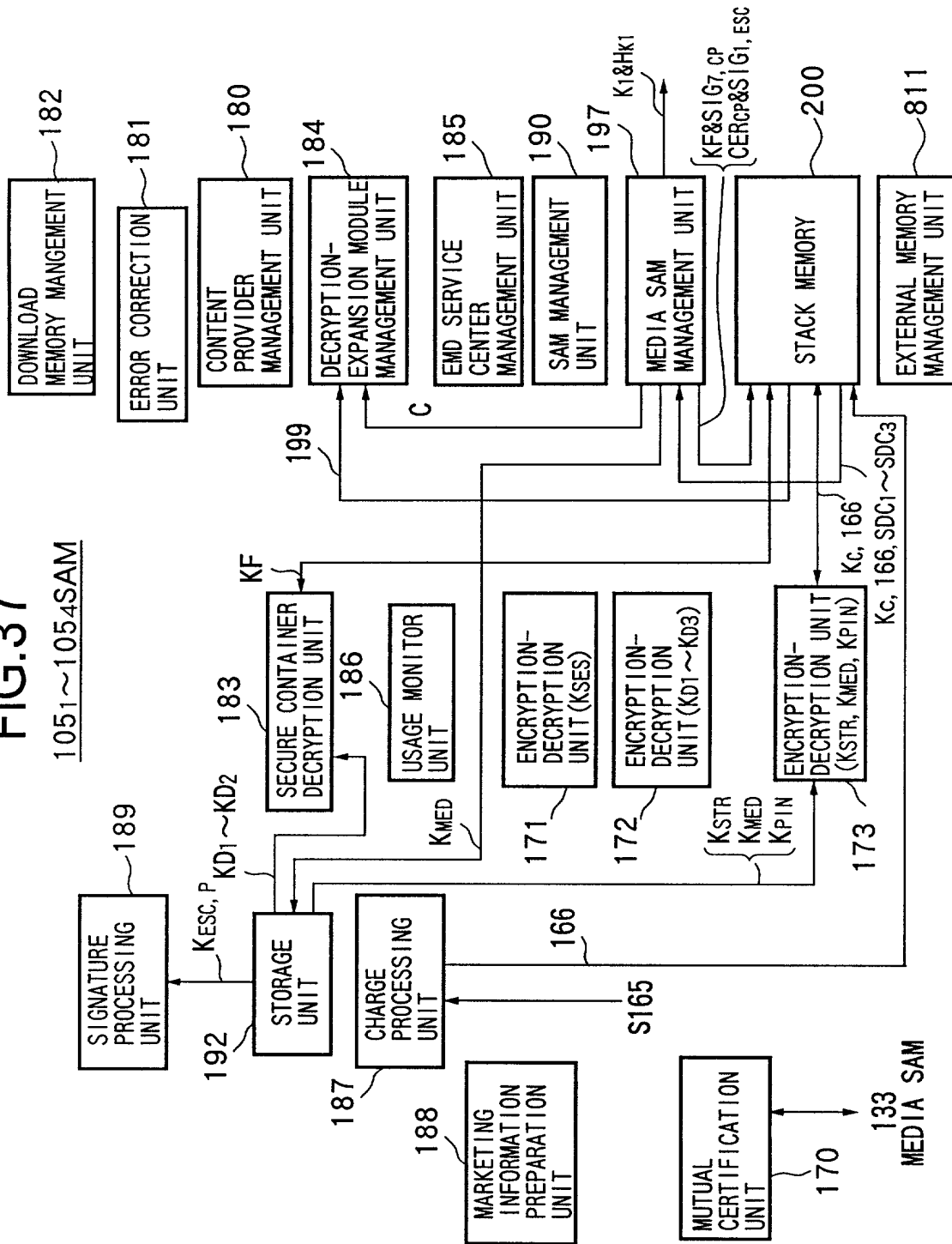


FIG.38

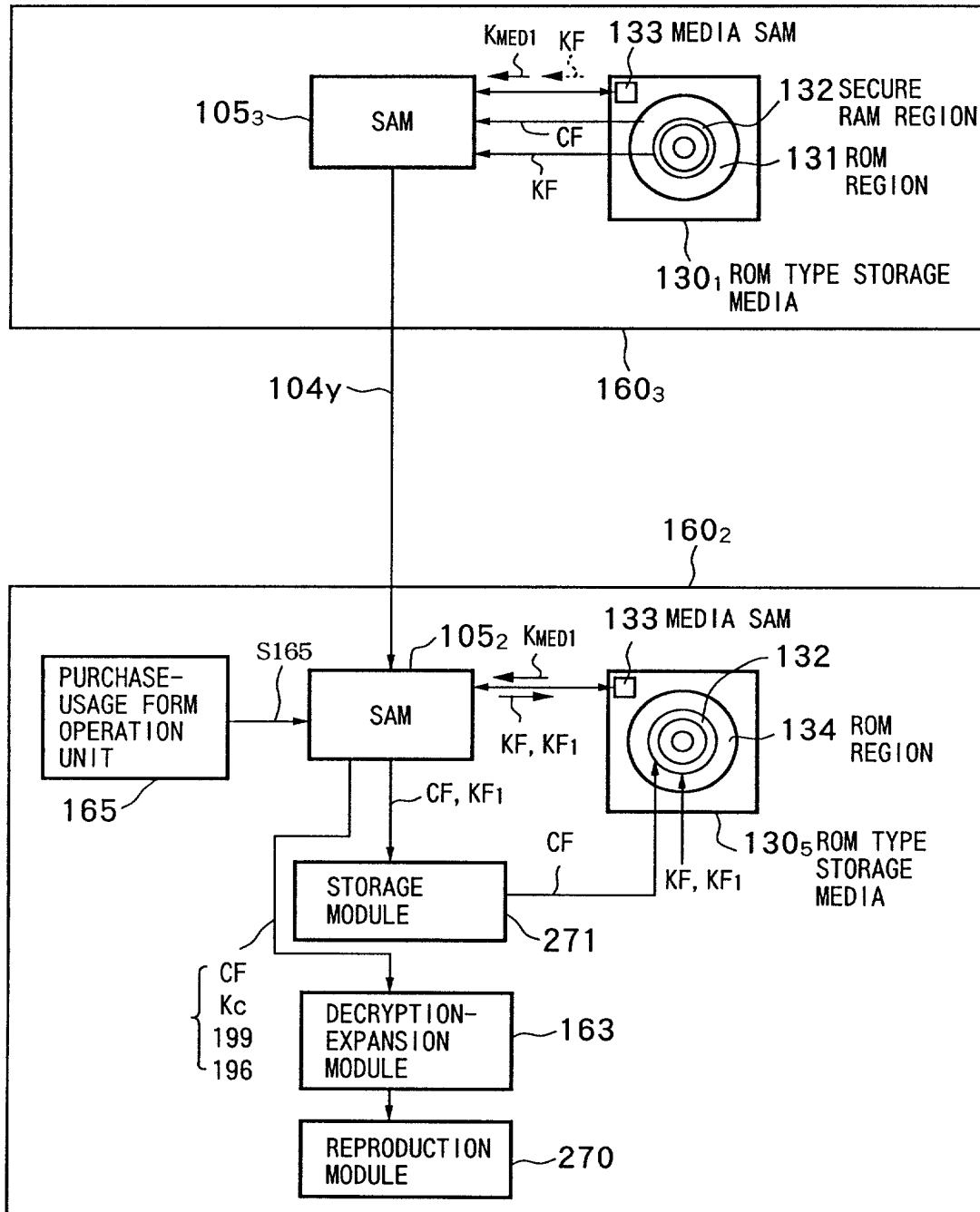
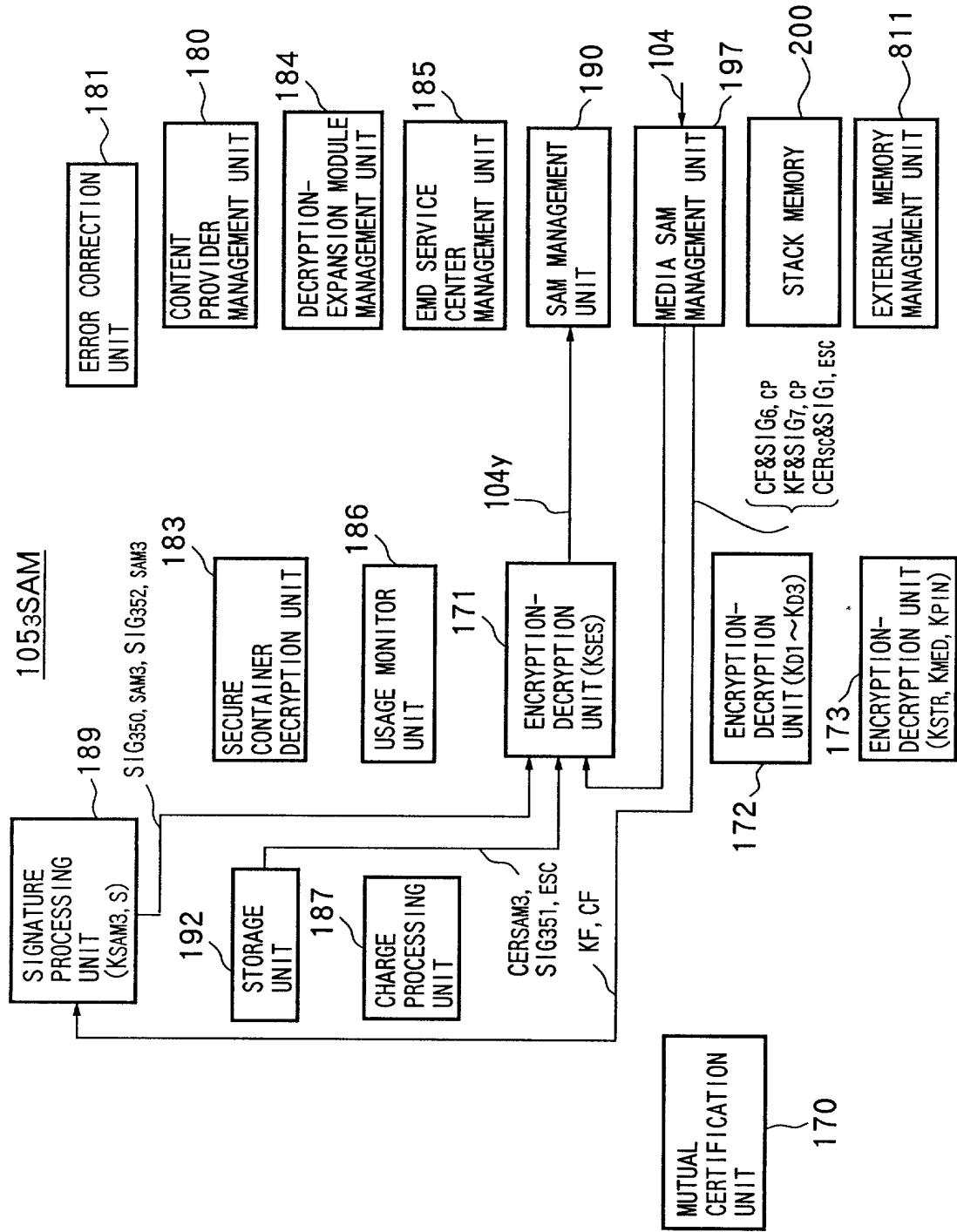


FIG. 39



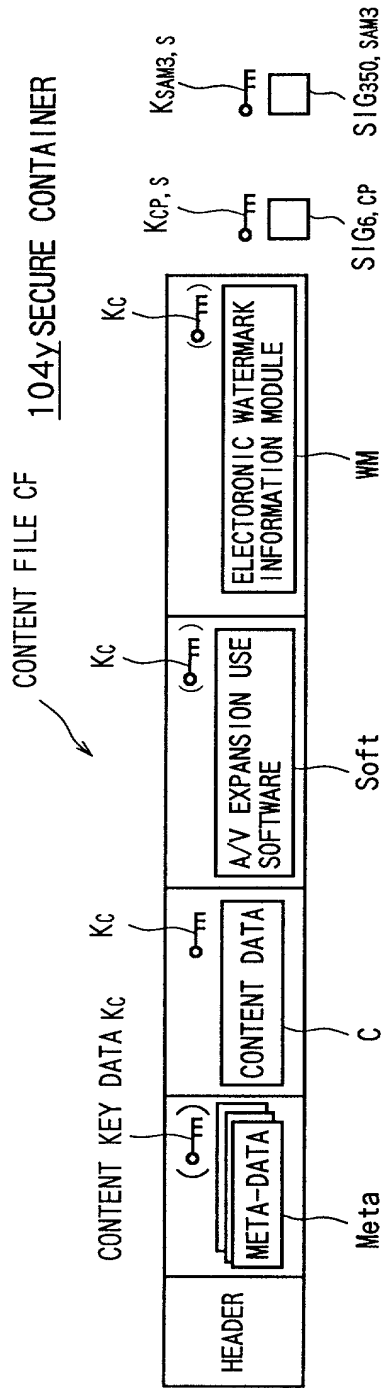


FIG. 40A

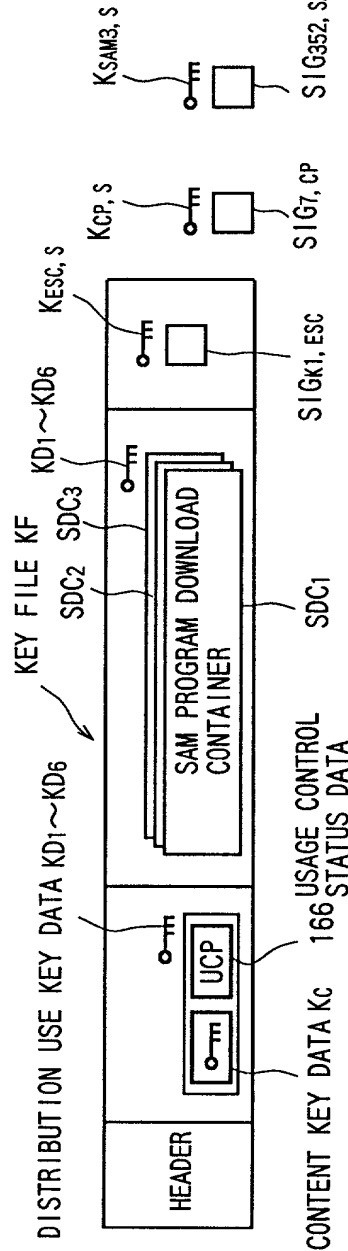


FIG. 40B

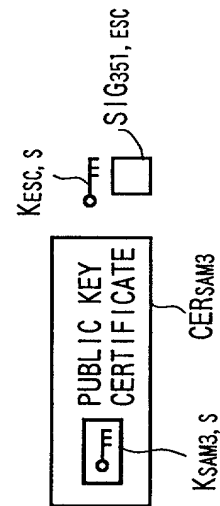


FIG. 40C

FIG. 41  
1052SAM

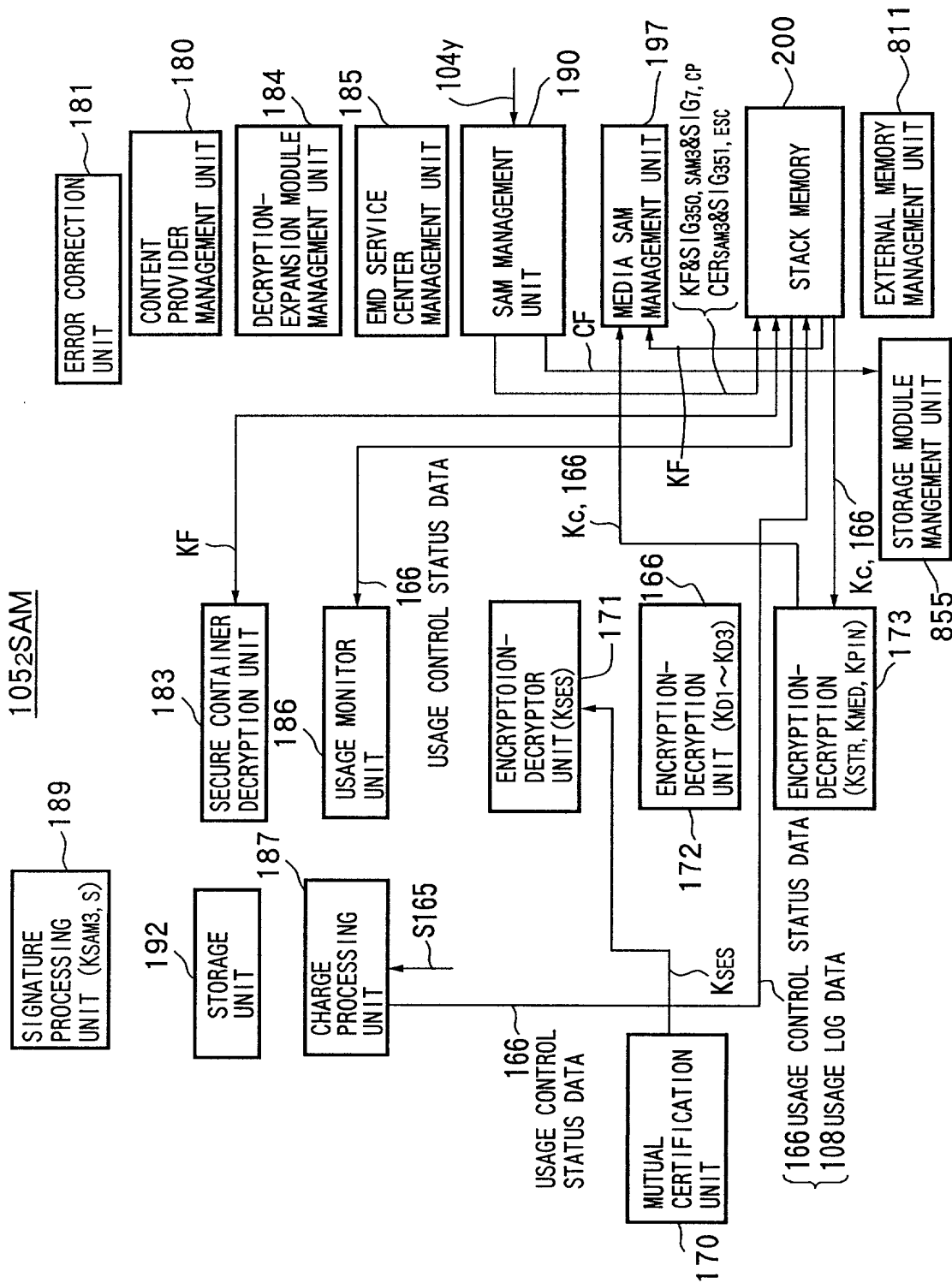


FIG.42A 101 (CP) → SAM105<sub>1</sub>  
(IN-BAND)

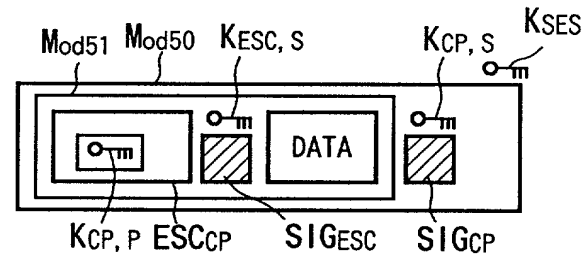


FIG.42B 101 (CP) → SAM105<sub>1</sub>  
(OUT-OF-BAND)

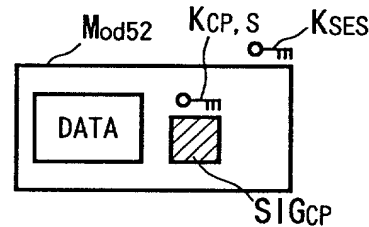


FIG.42C 102 (ESC) → SAM105<sub>1</sub>  
(OUT-OF-BAND)

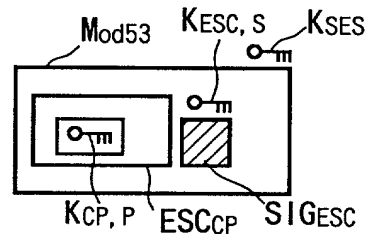


FIG.42D SAM105<sub>1</sub> → 101 (CP)  
(IN-BAND)

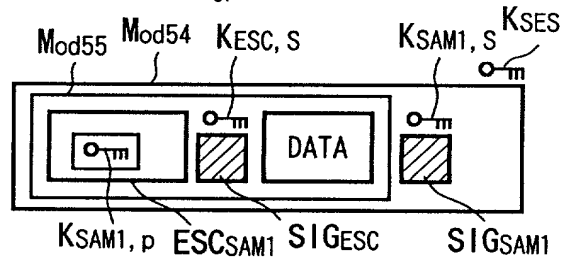


FIG.42E SAM105<sub>1</sub> → 101 (CP)  
(OUT-OF-BAND)

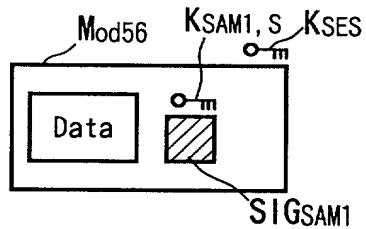


FIG.42F 102 (ESC) → 101 (CP)  
(OUT-OF-BAND)

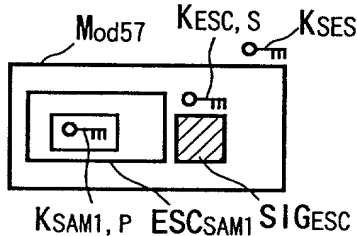


FIG.43G 101 (CP) → 102 (ESC)  
(IN-BAND)

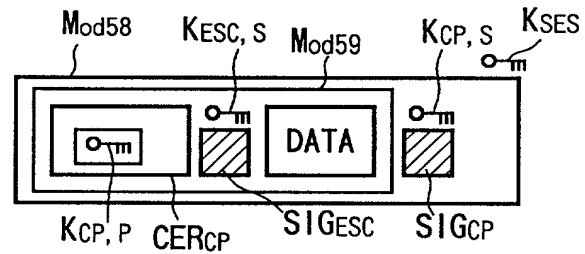


FIG.43H 101 (CP) → 102 (ESC)  
(OUT-OF-BAND)

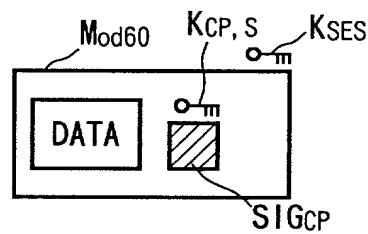


FIG.43I SAM105<sub>1</sub> → 102 (ESC)  
(IN-BAND)

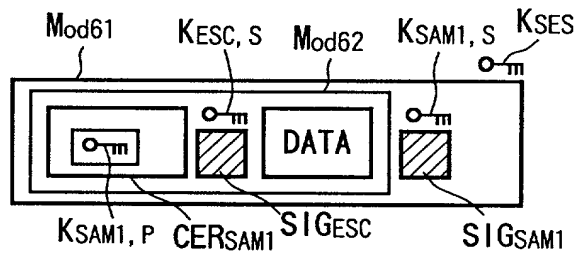


FIG.43J SAM105<sub>1</sub> → 102 (ESC)  
(OUT-OF-BAND)

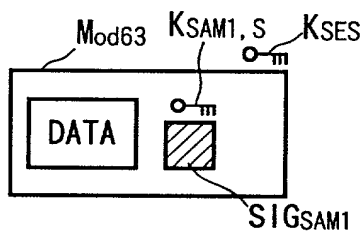


FIG.44

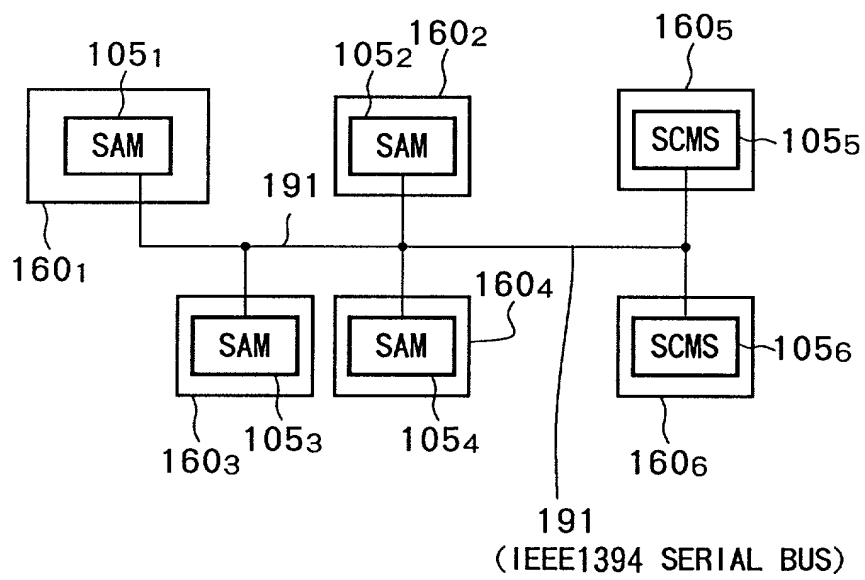




FIG.45

SAM REGISTRATION LIST (PREPARED BY SAM)

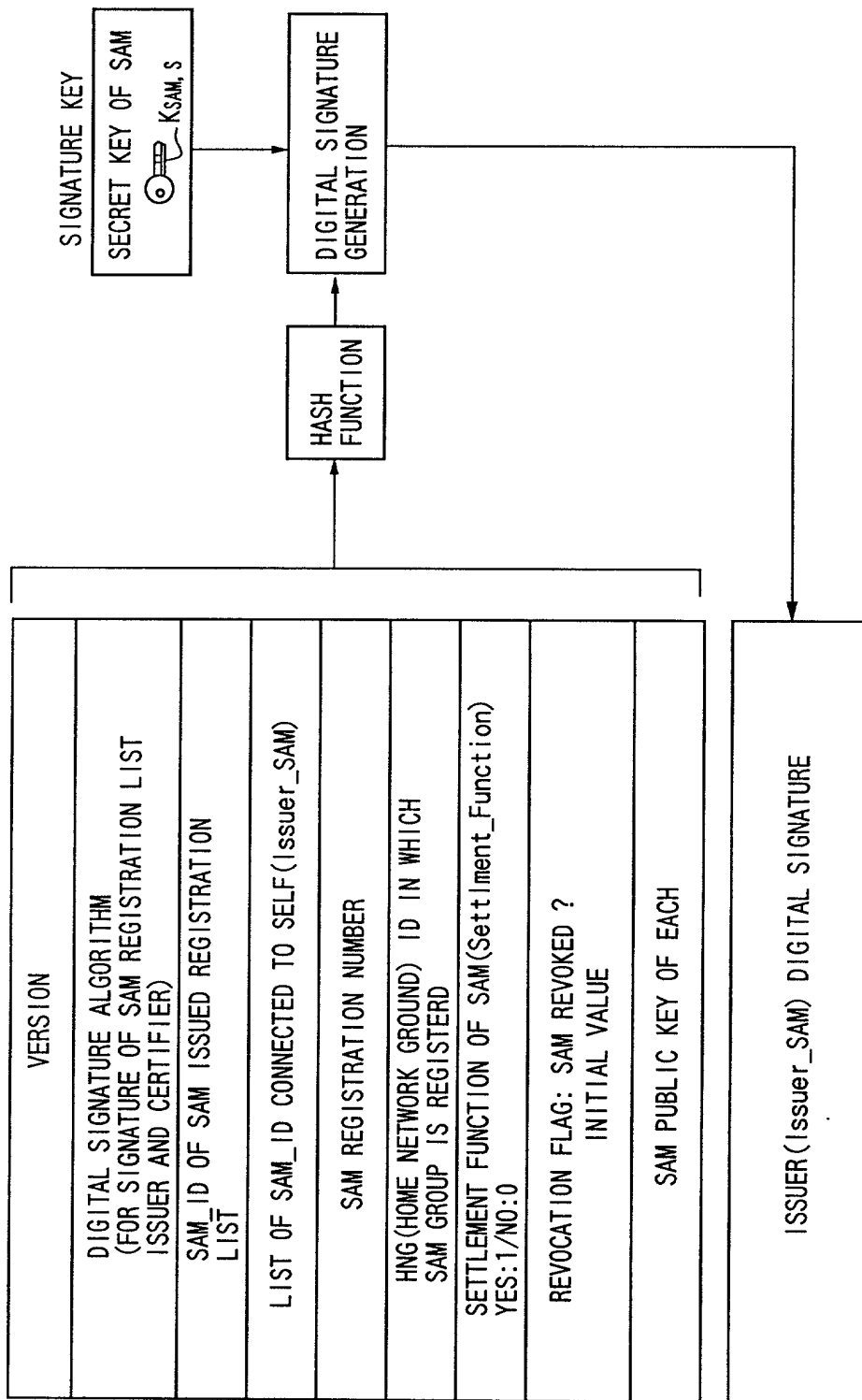


FIG.46

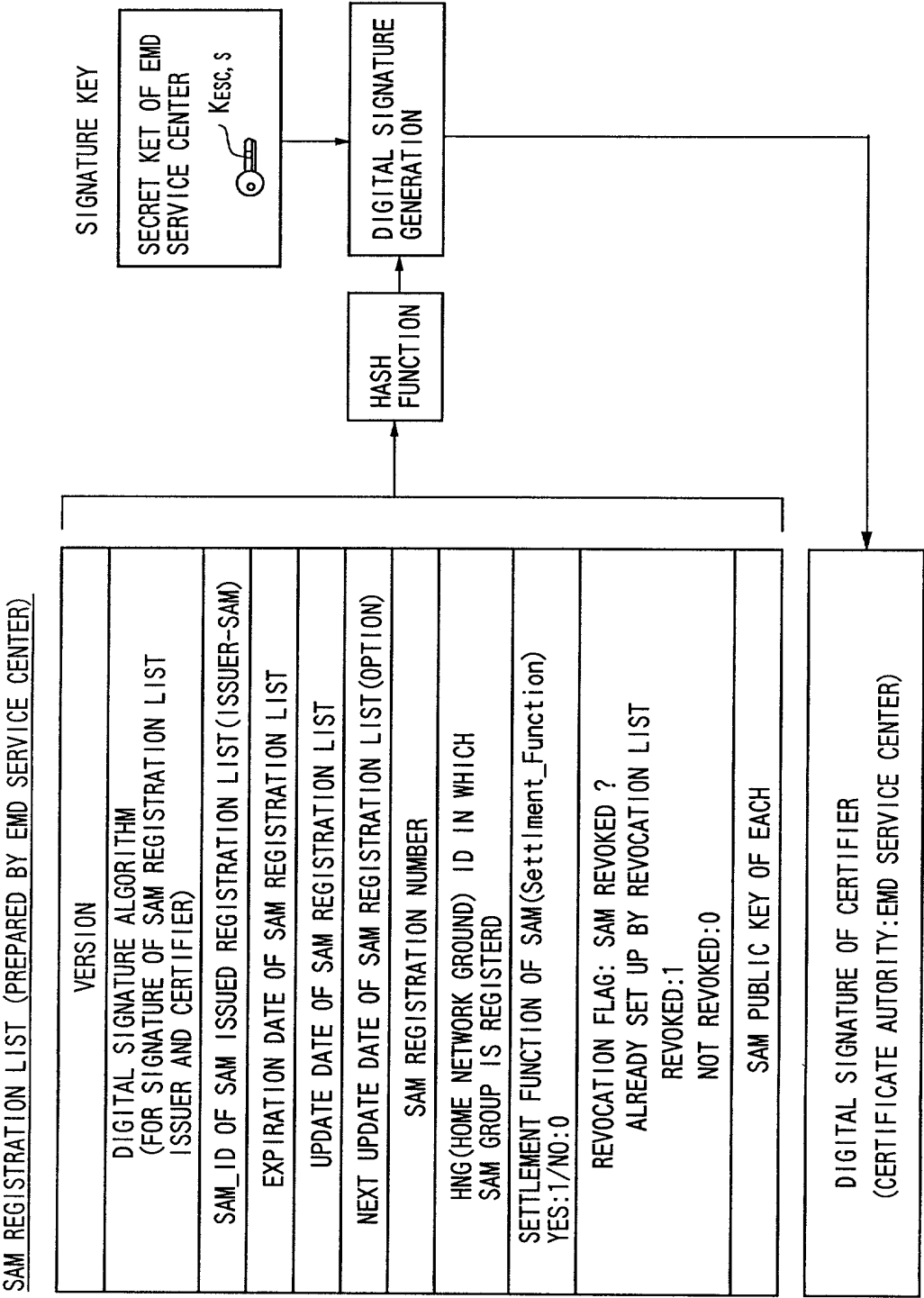
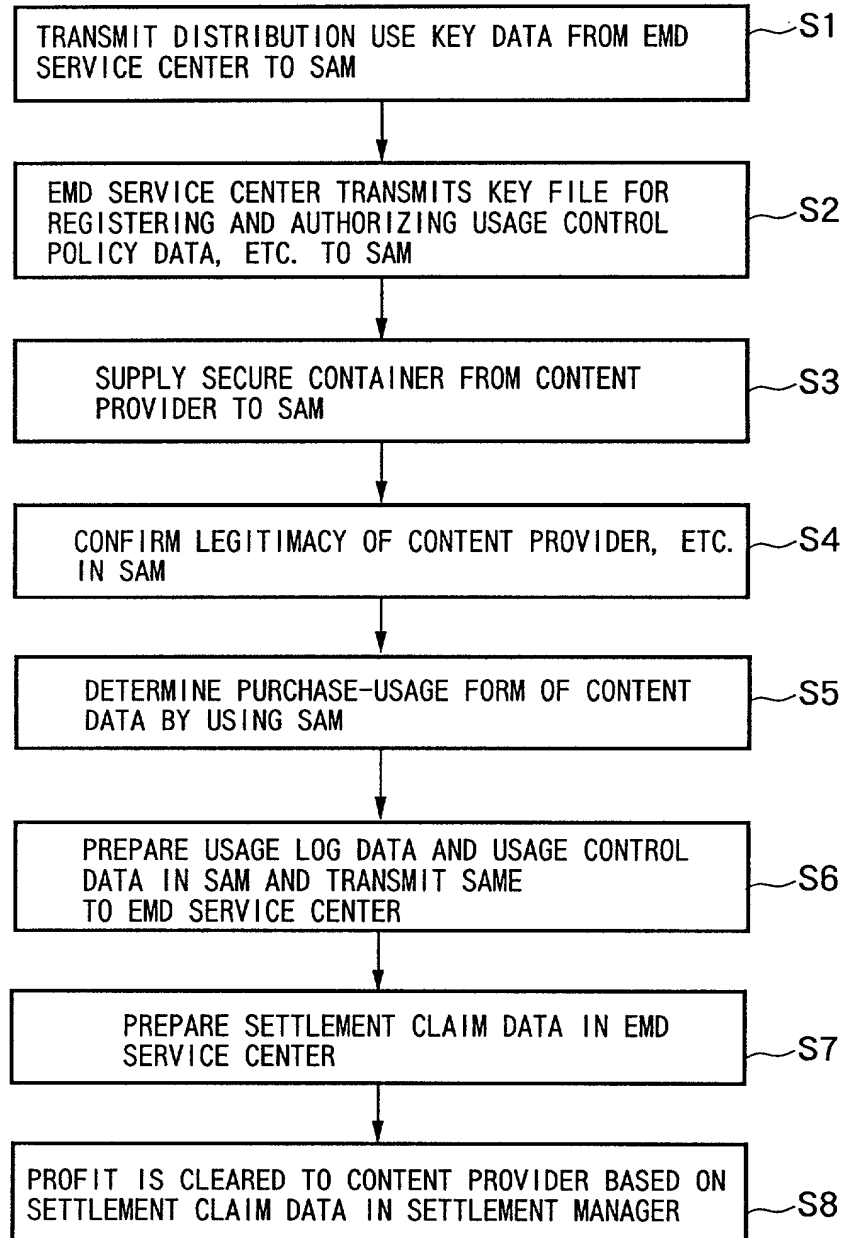


FIG.47



[illegible]

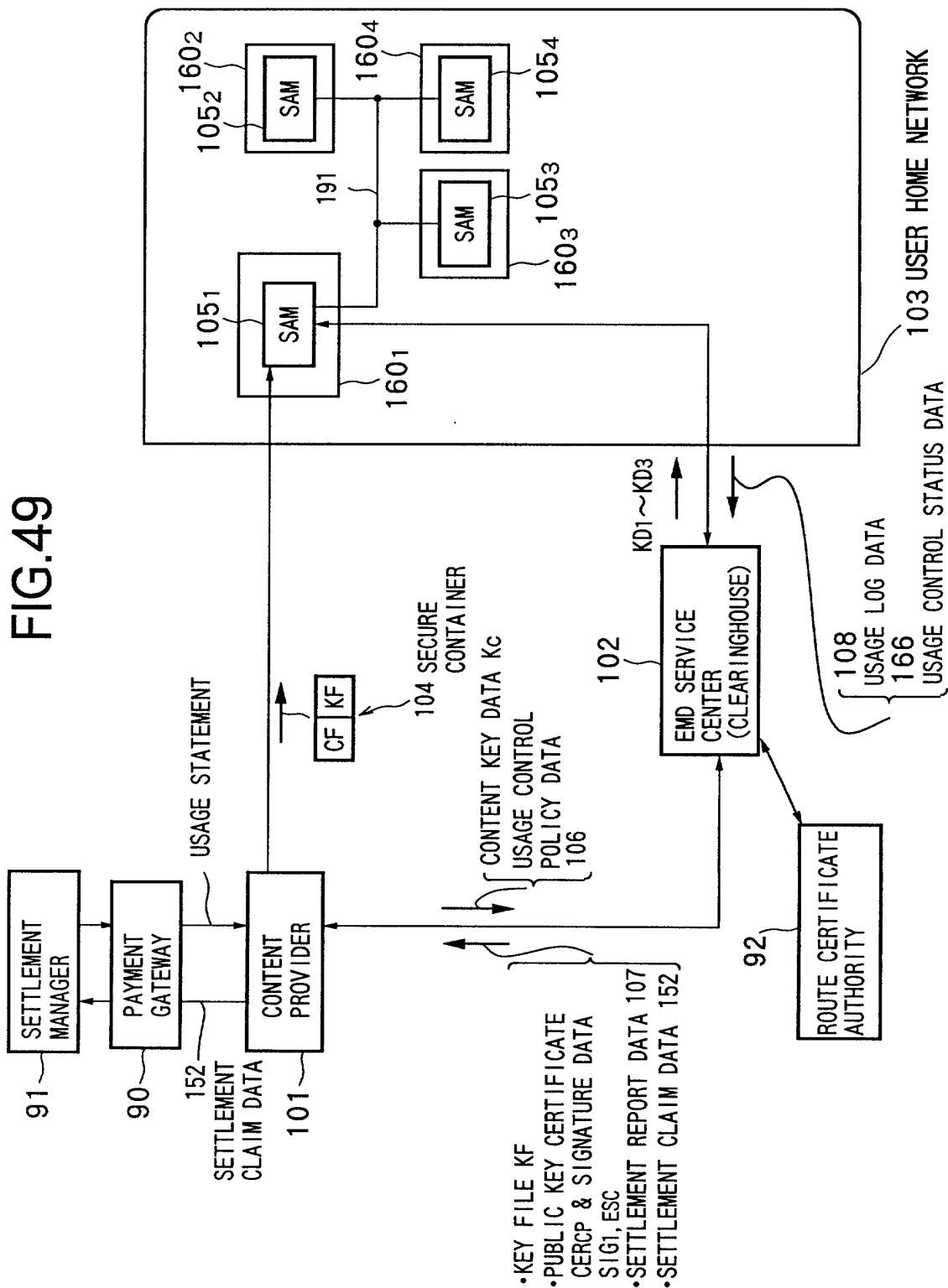


FIG. 50

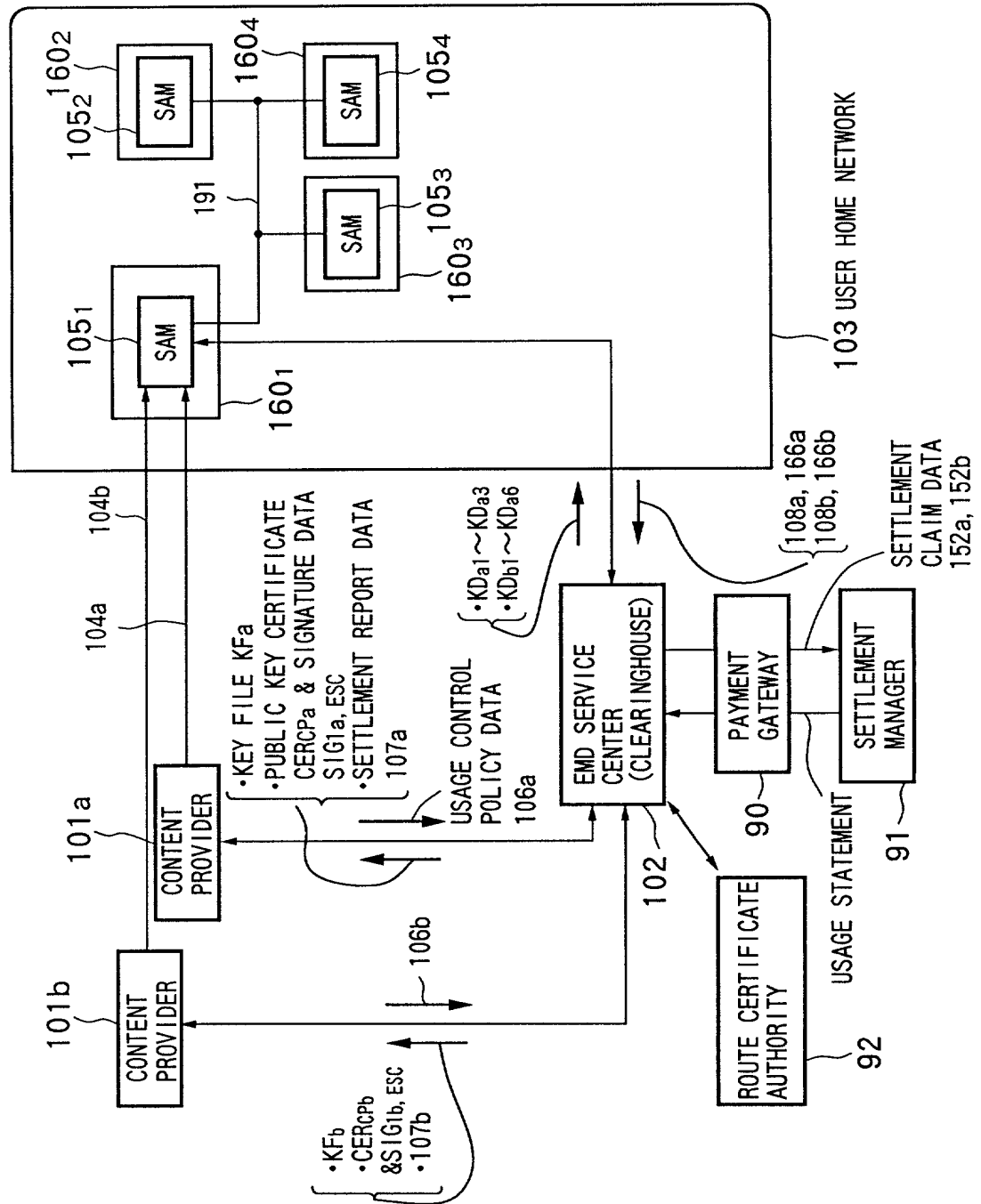
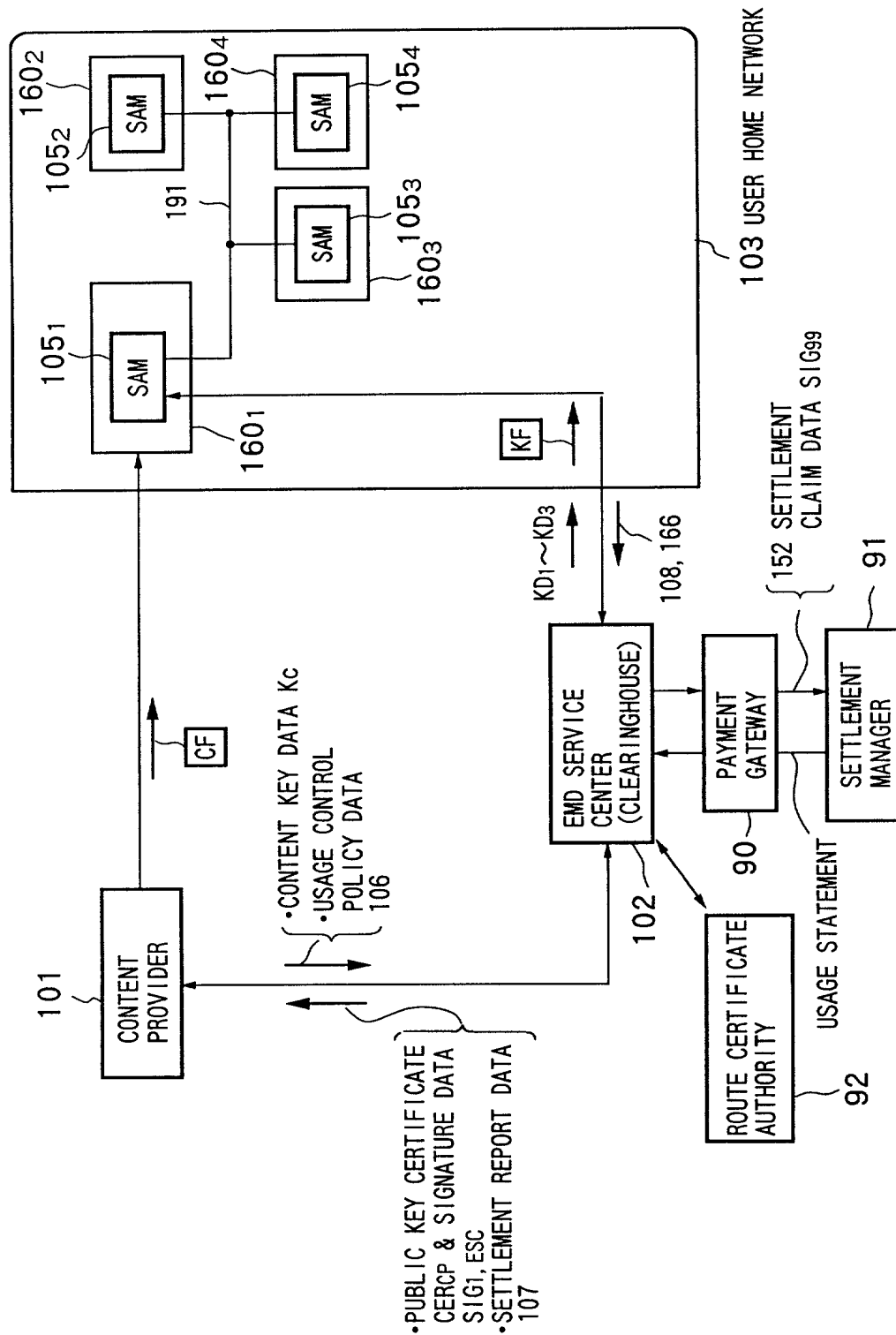




FIG. 52





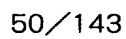


FIG. 54

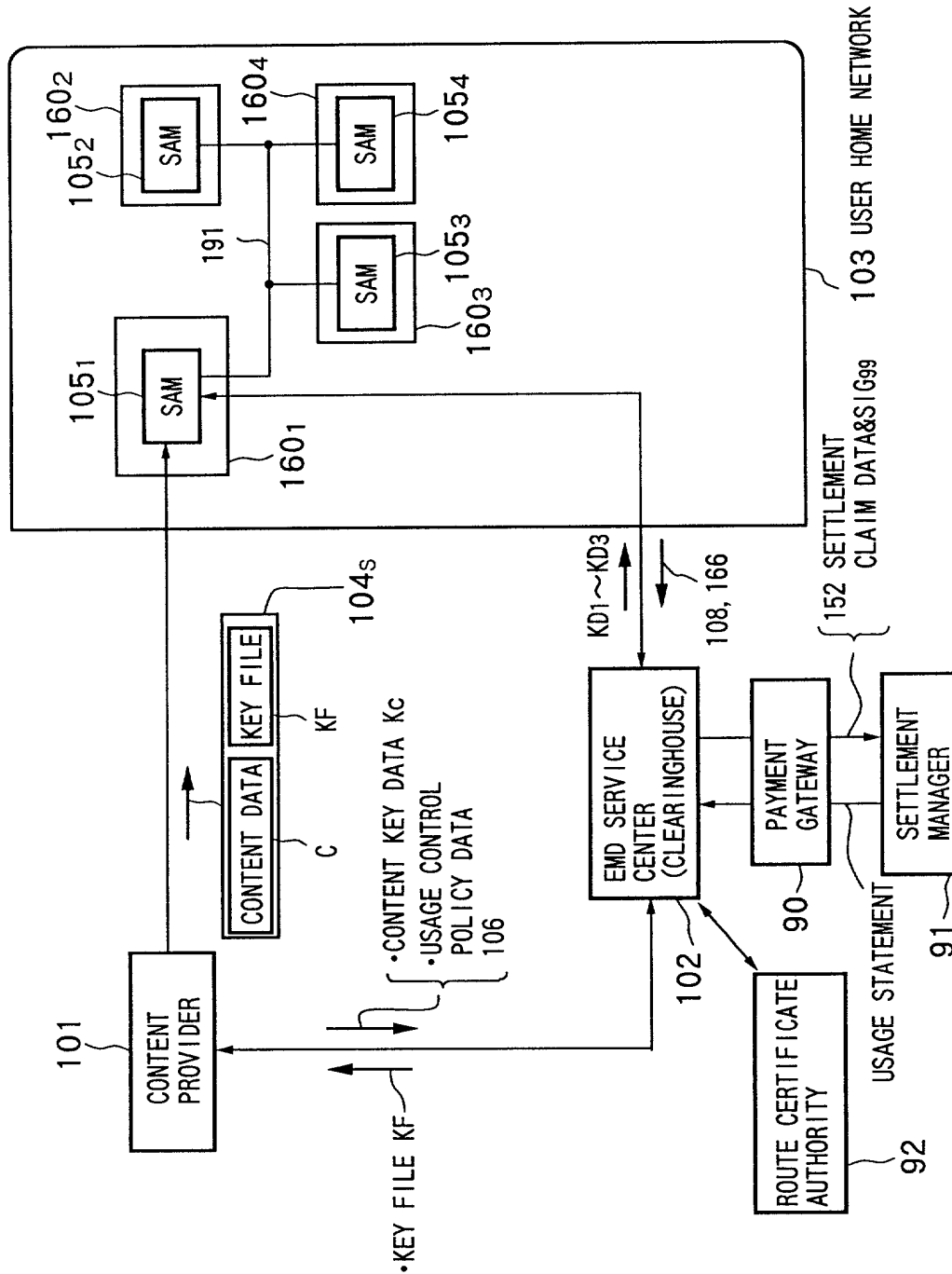




FIG.56

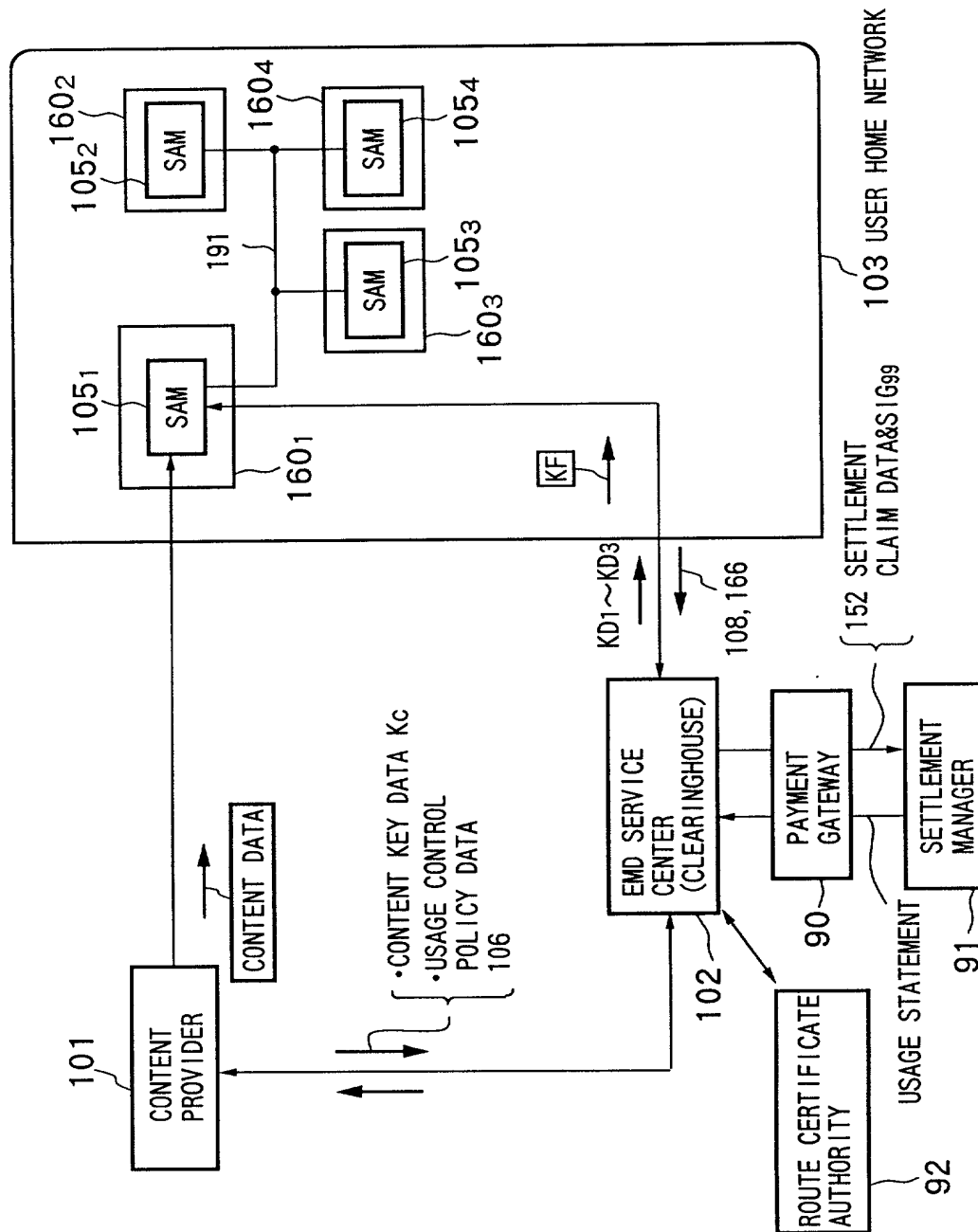


FIG. 57

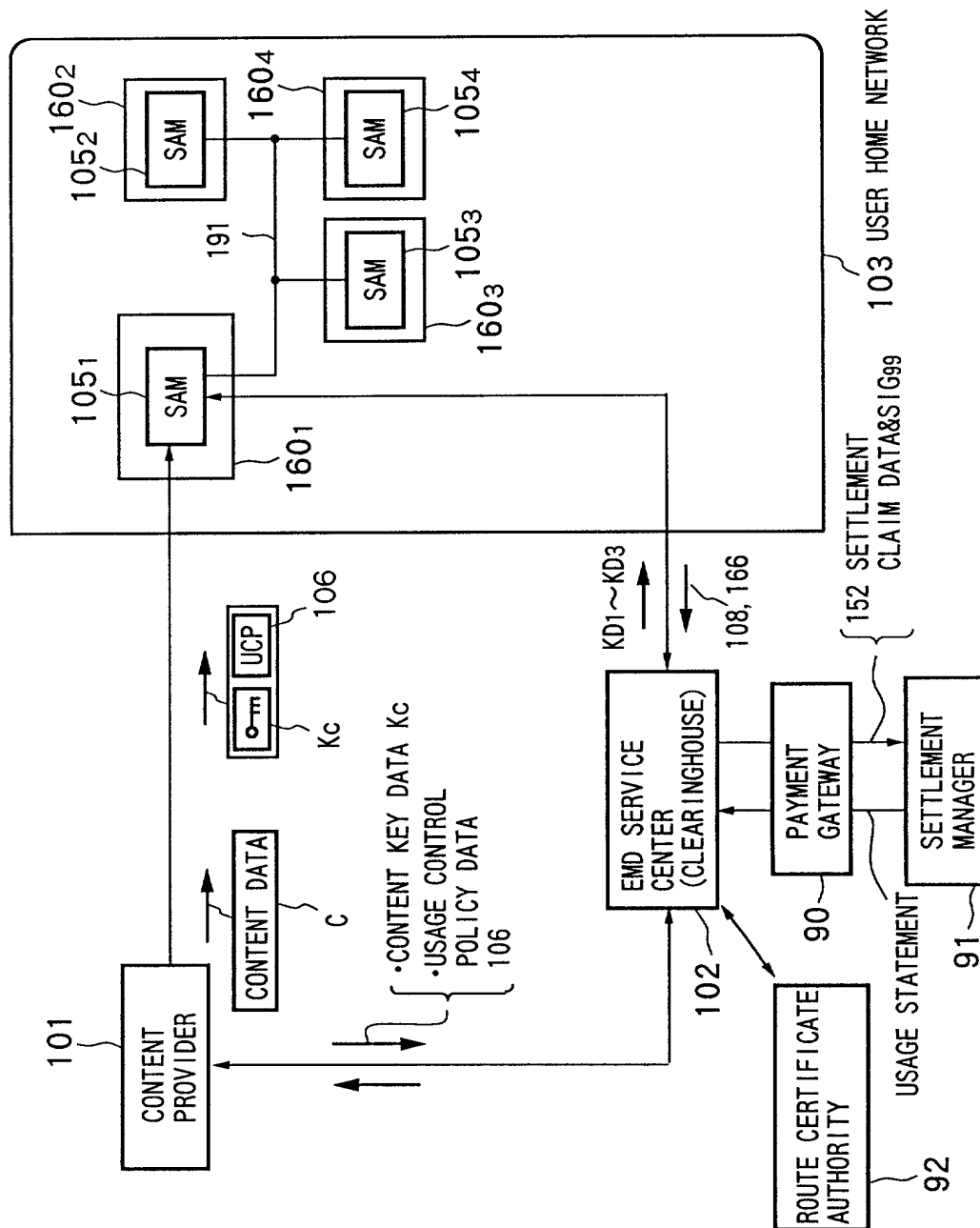


FIG. 58

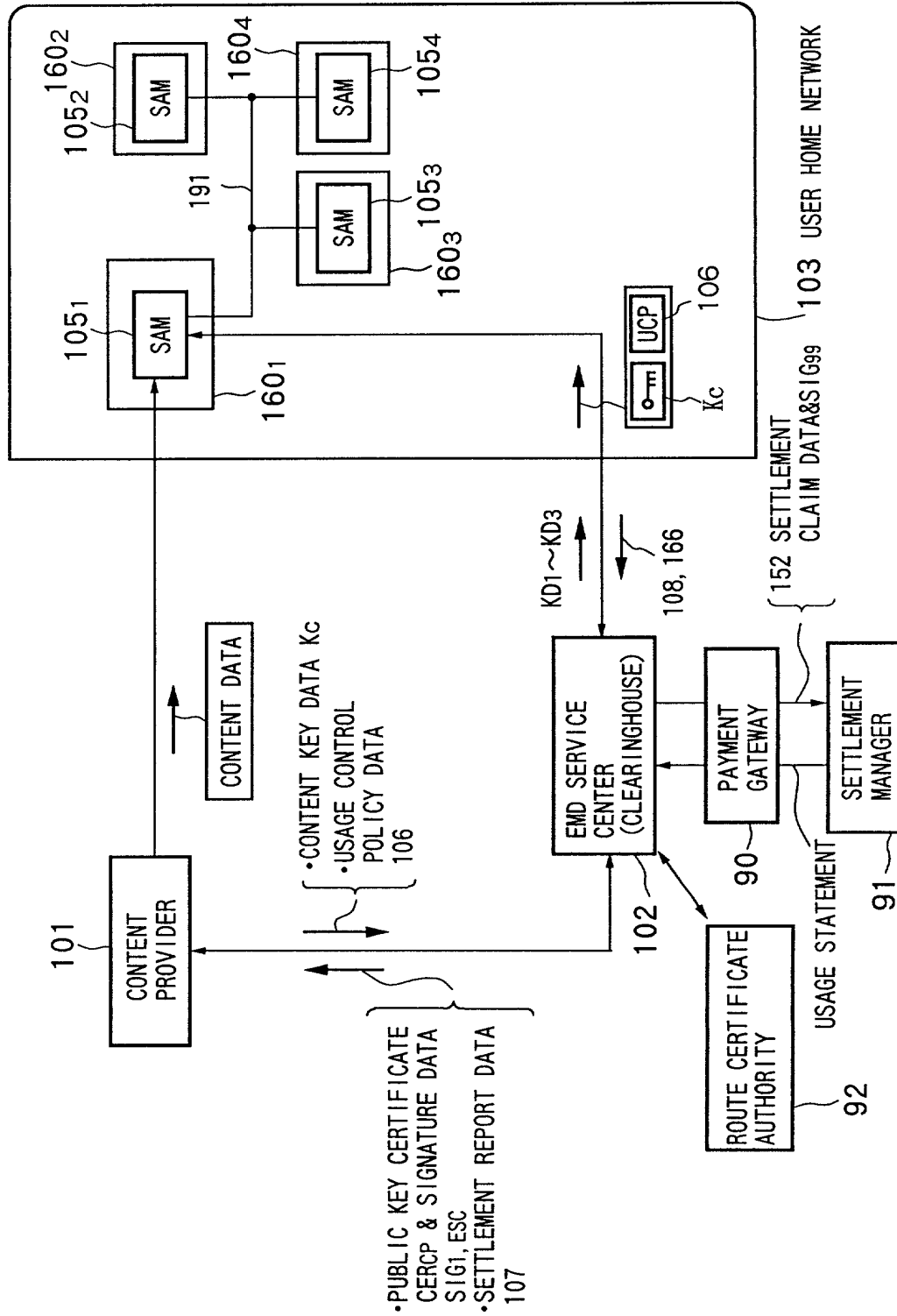
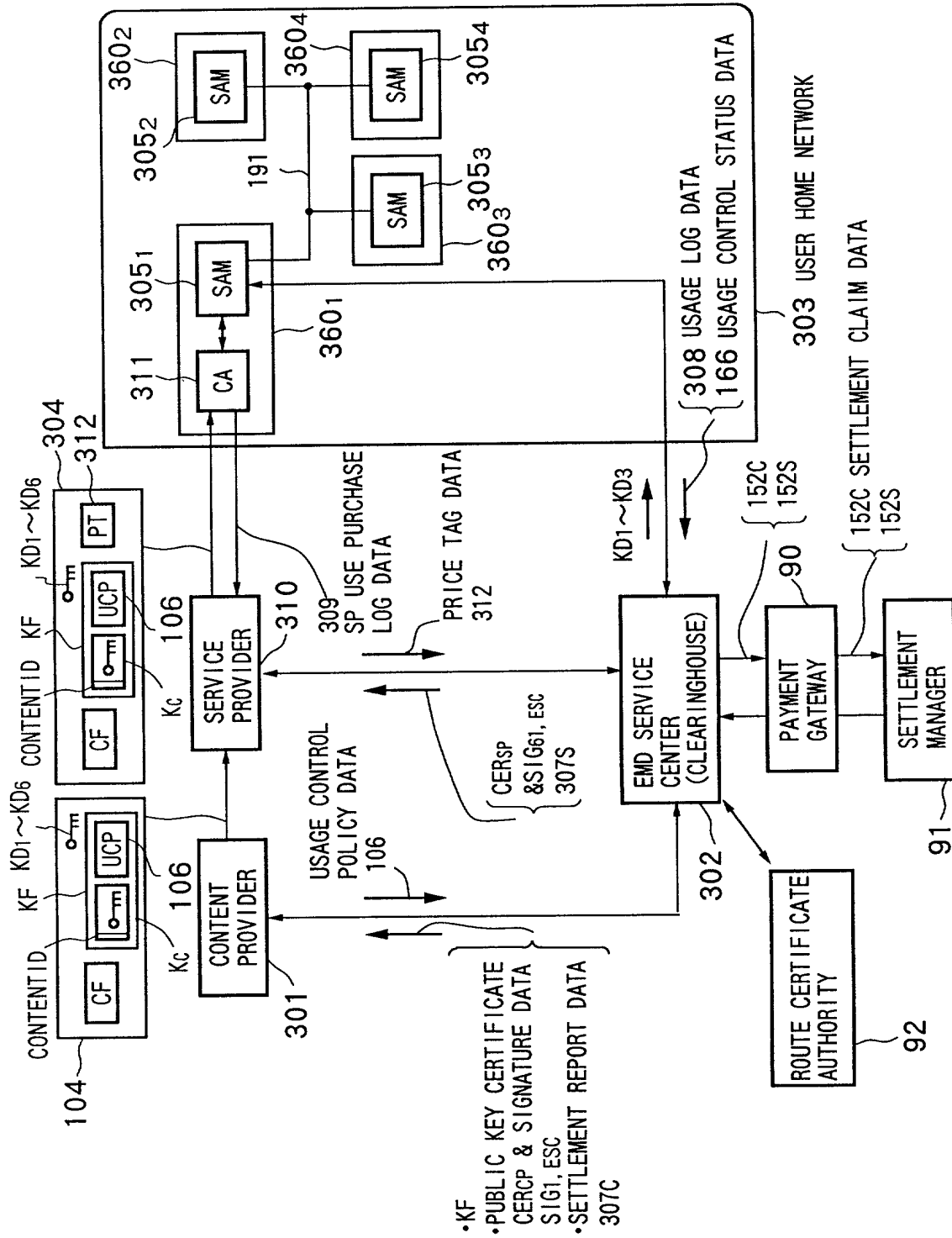


FIG. 59



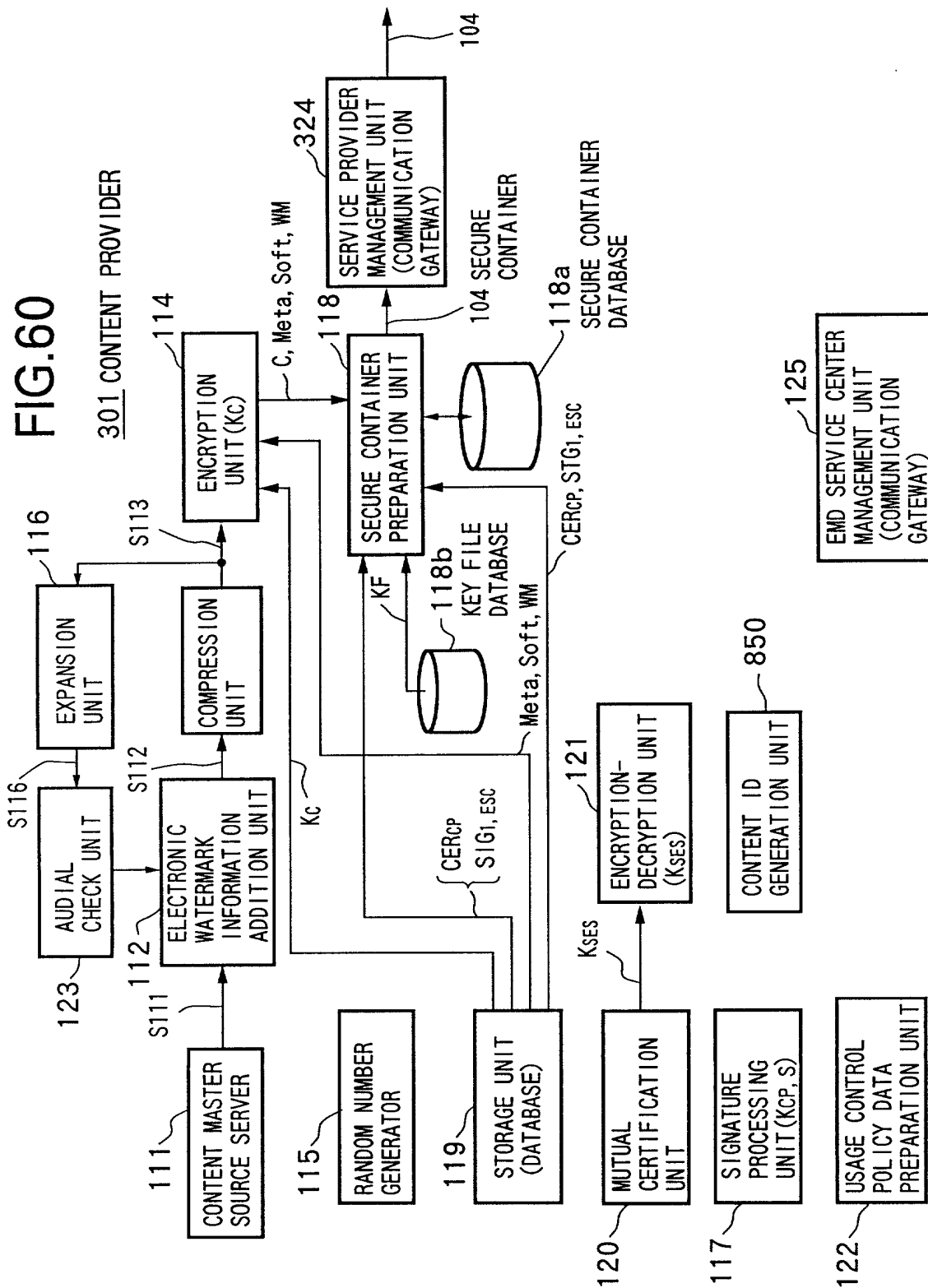




FIG.61

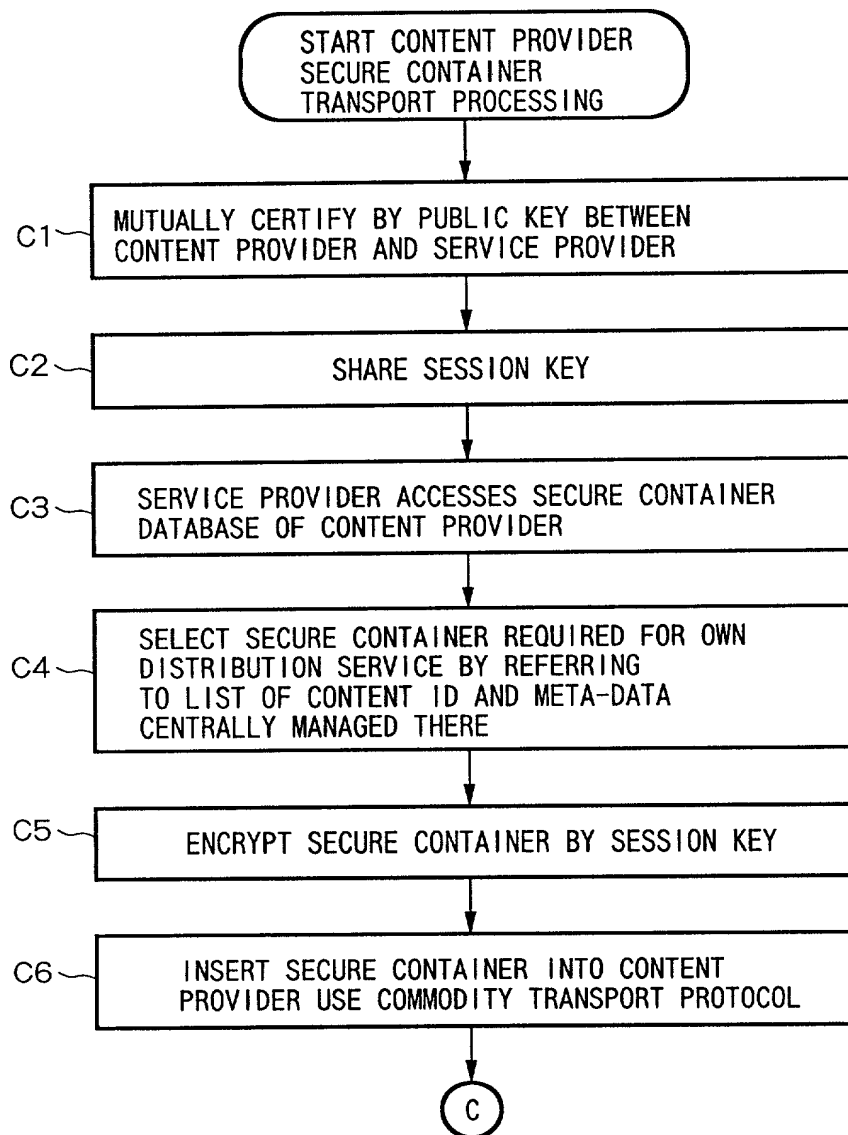


FIG.62

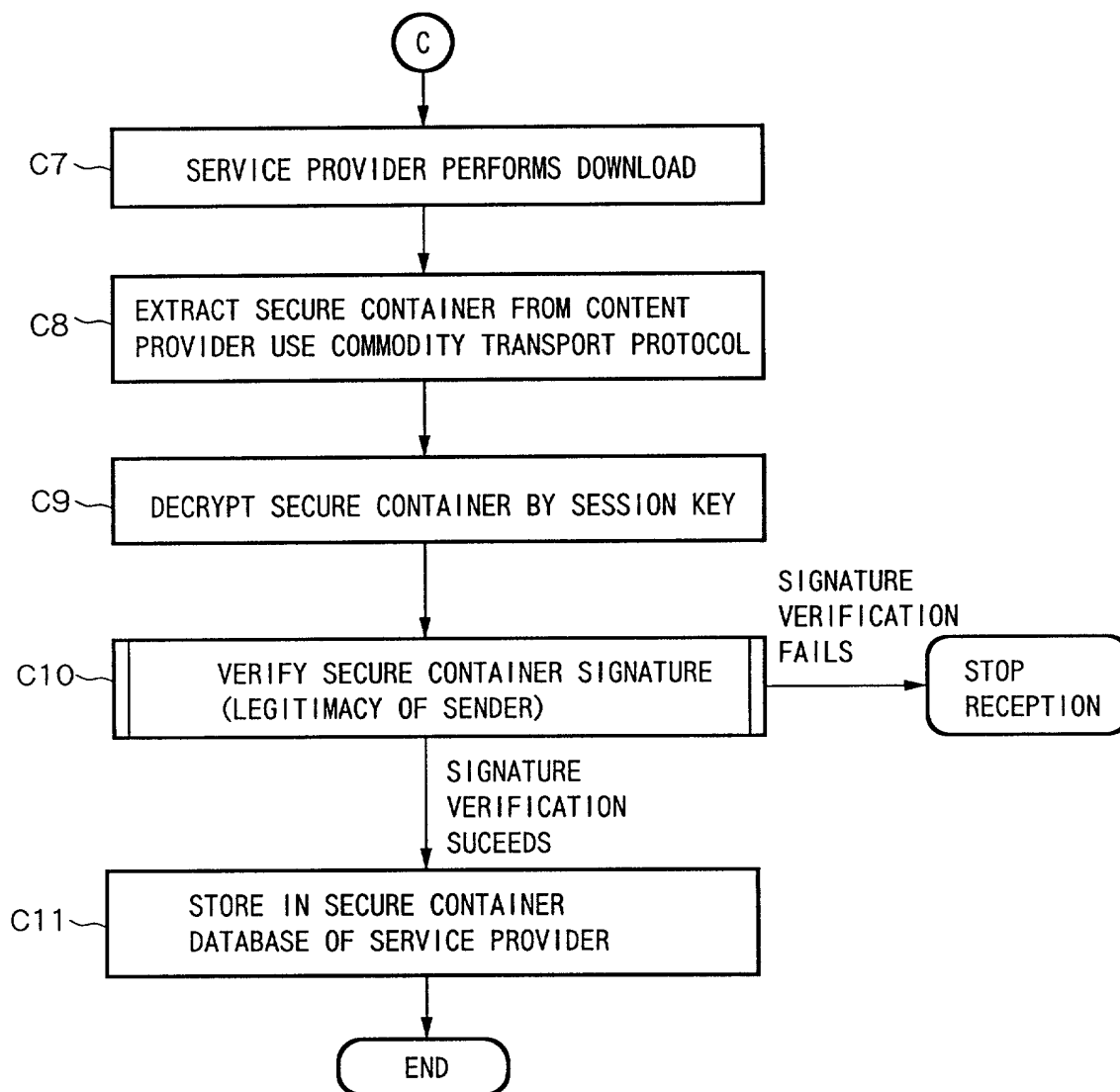


FIG. 63

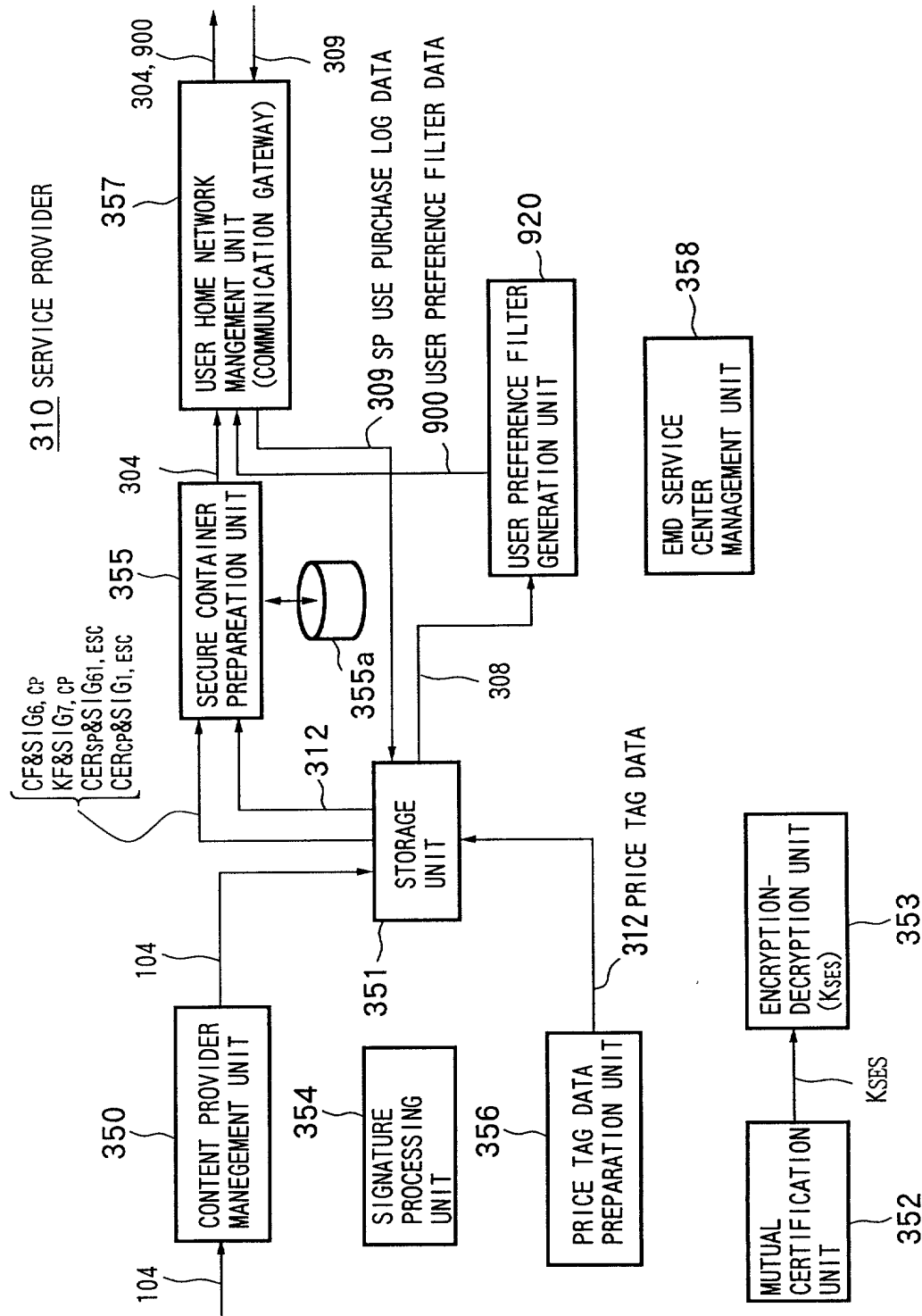
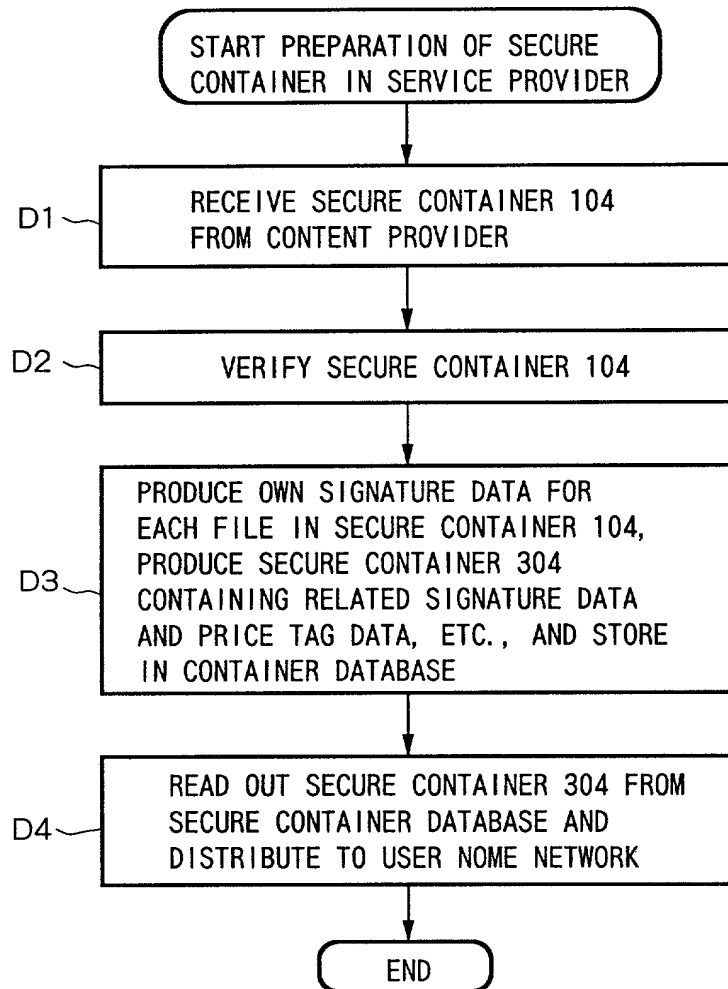


FIG.64



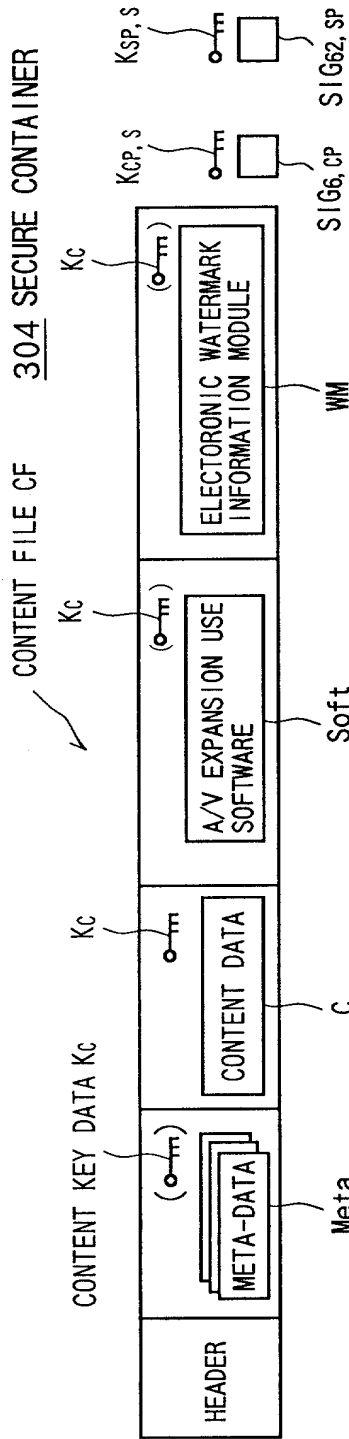


FIG. 65A

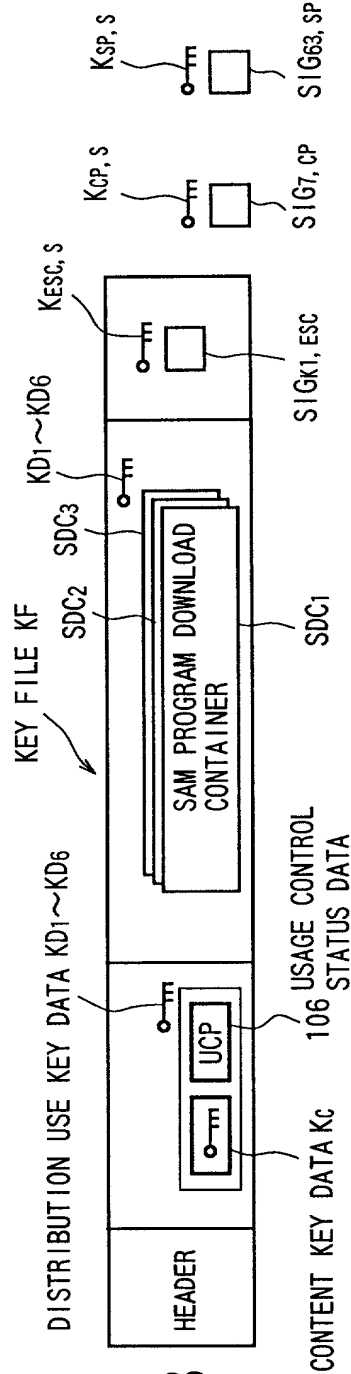


FIG. 65B

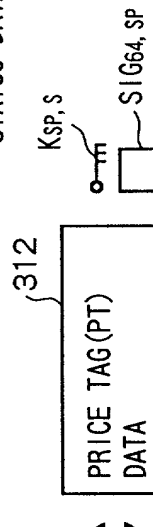


FIG. 65C

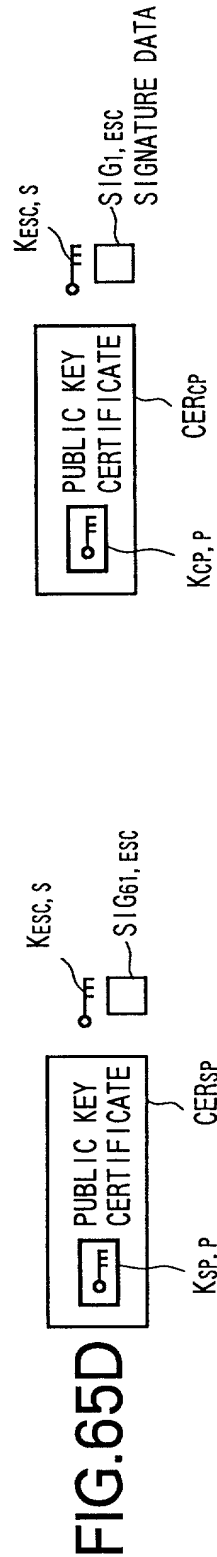
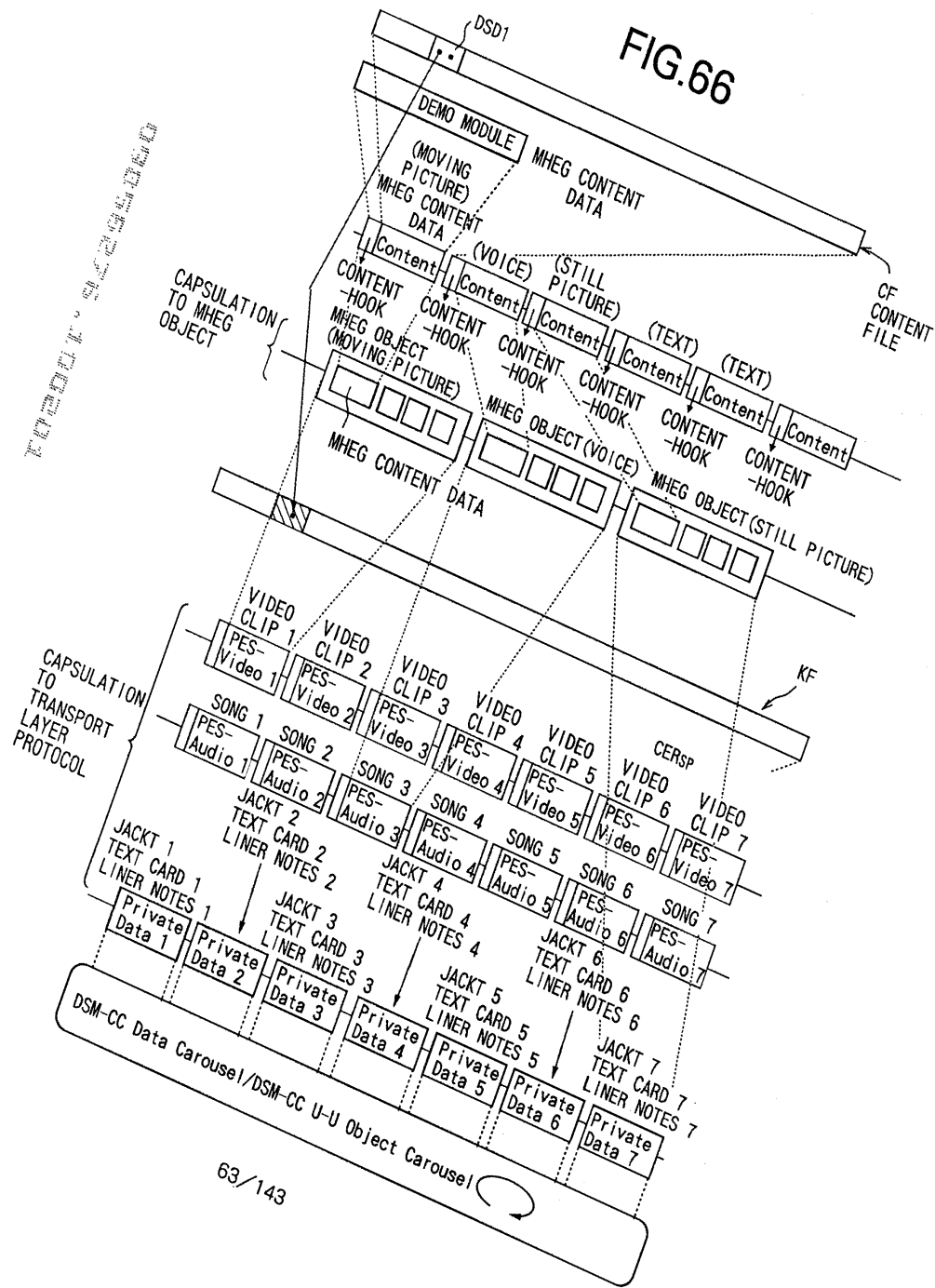


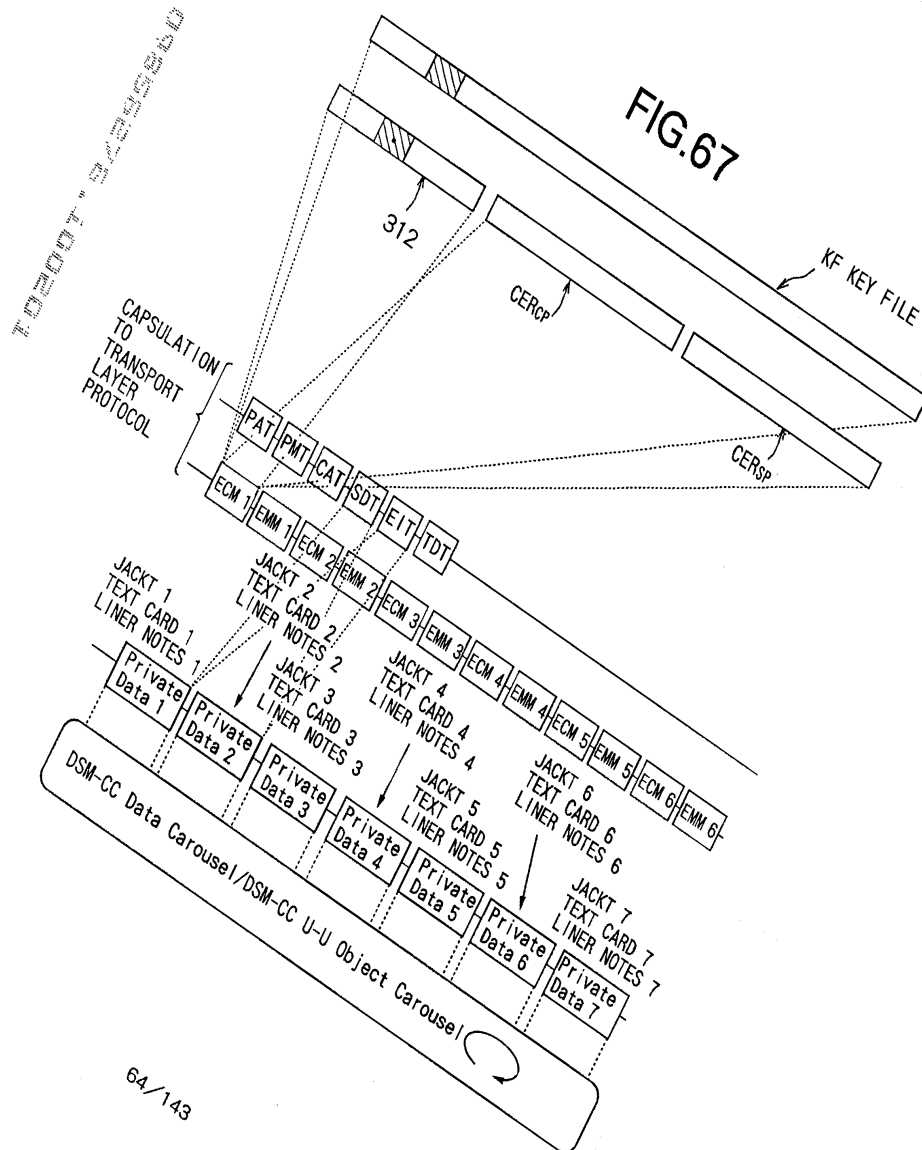
FIG. 65D

09/856276

FIG.66



09/856276



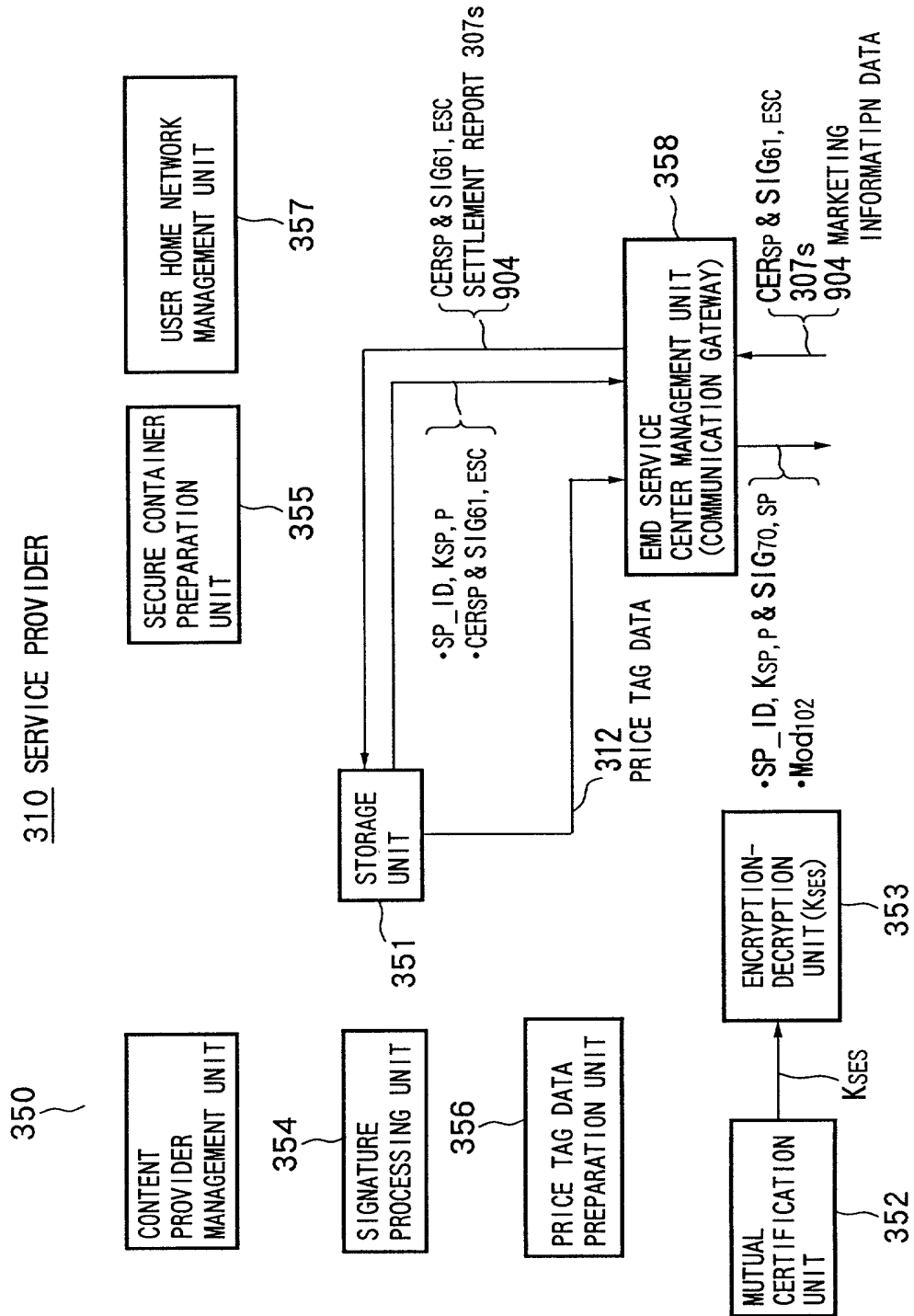
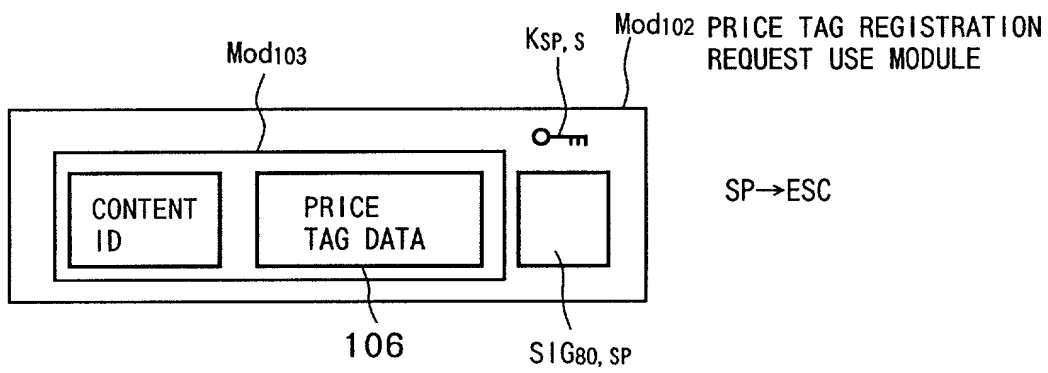




FIG.69



**FIG. 70**

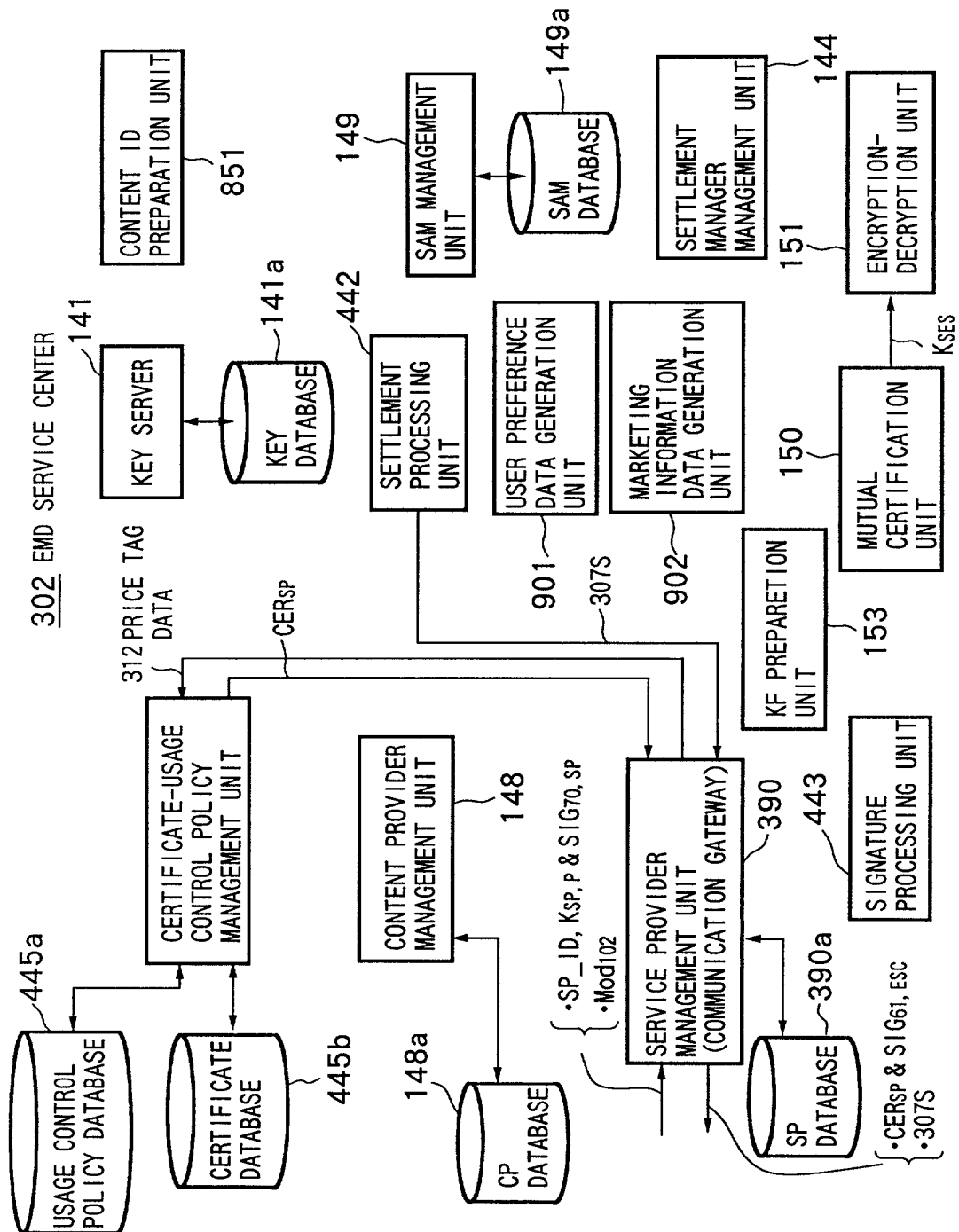


FIG. 71

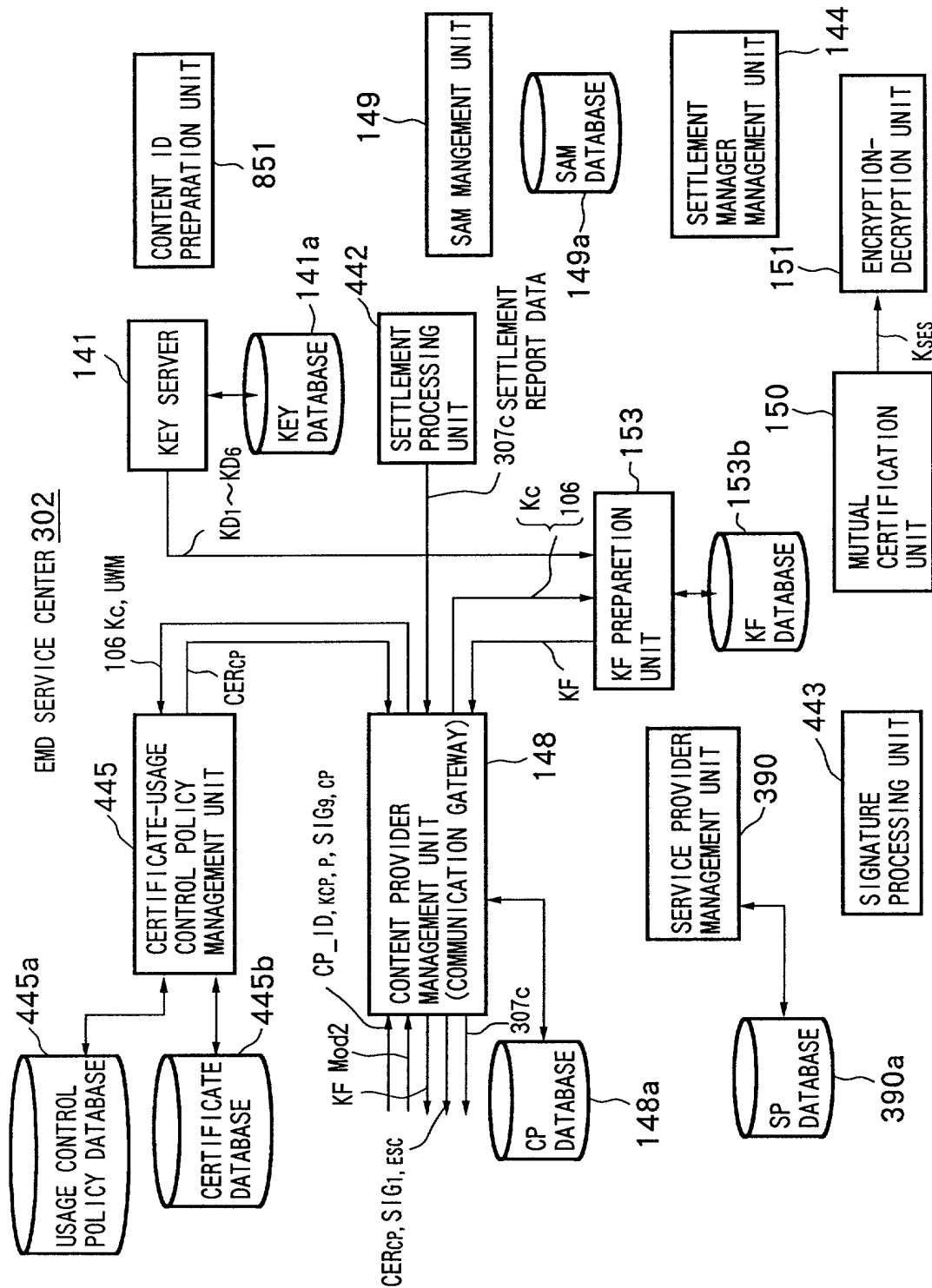
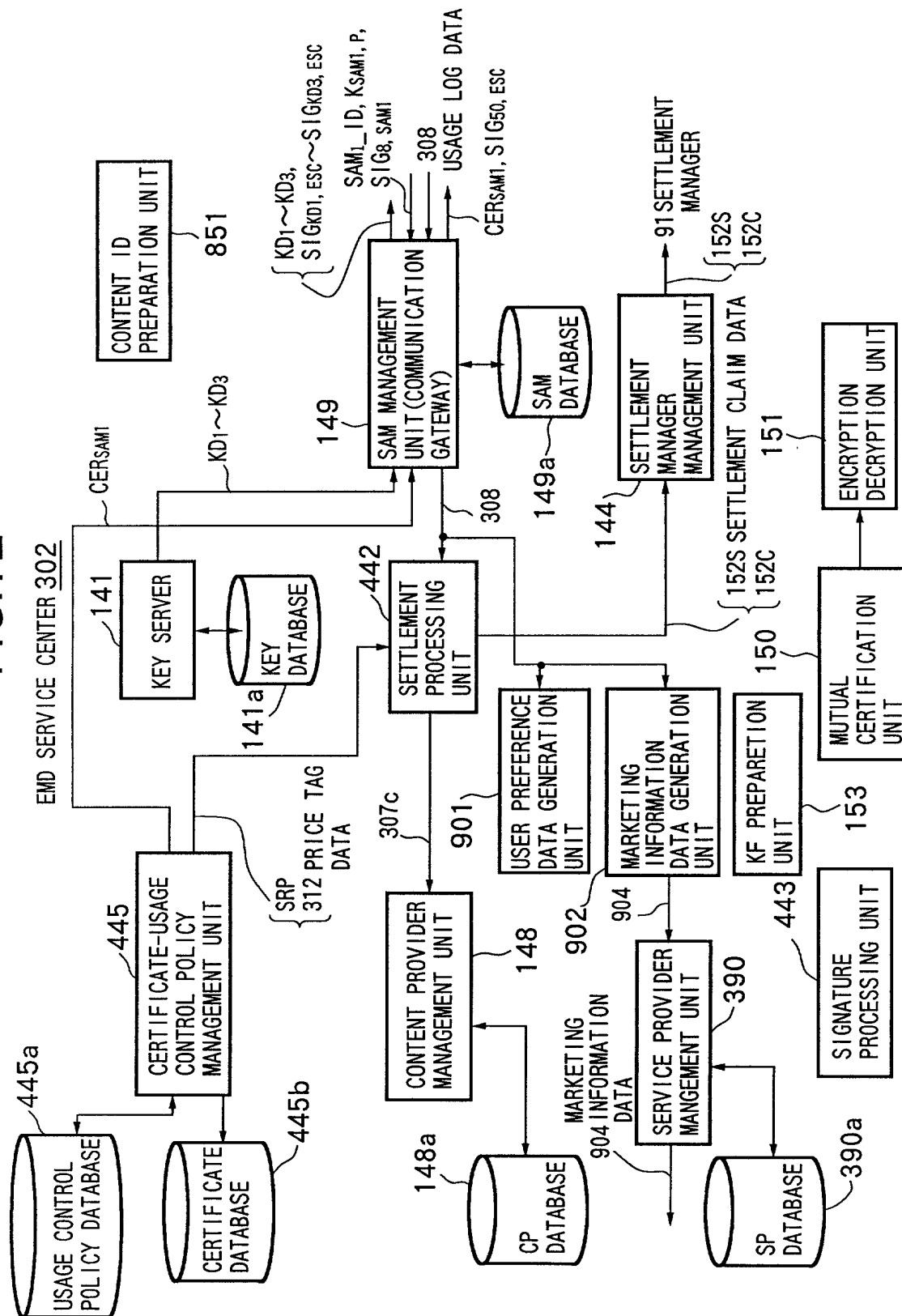


FIG. 72



**FIG.73****CONTENT OF USAGE LOG DATA 308**

IDENTIFIER Content\_ID  
IDENTIFIER CP\_ID  
IDENTIFIER SP\_ID  
SIGNAL PARAMETER DATA OF CONTENT DATA C  
COMPRESSION METHOD OF CONTENT DATA C  
IDENTIFIER MEDIA\_ID OF STORAGE MEDIA  
IDENTIFIER SAM\_ID  
USER\_ID OF USER

FIG.74

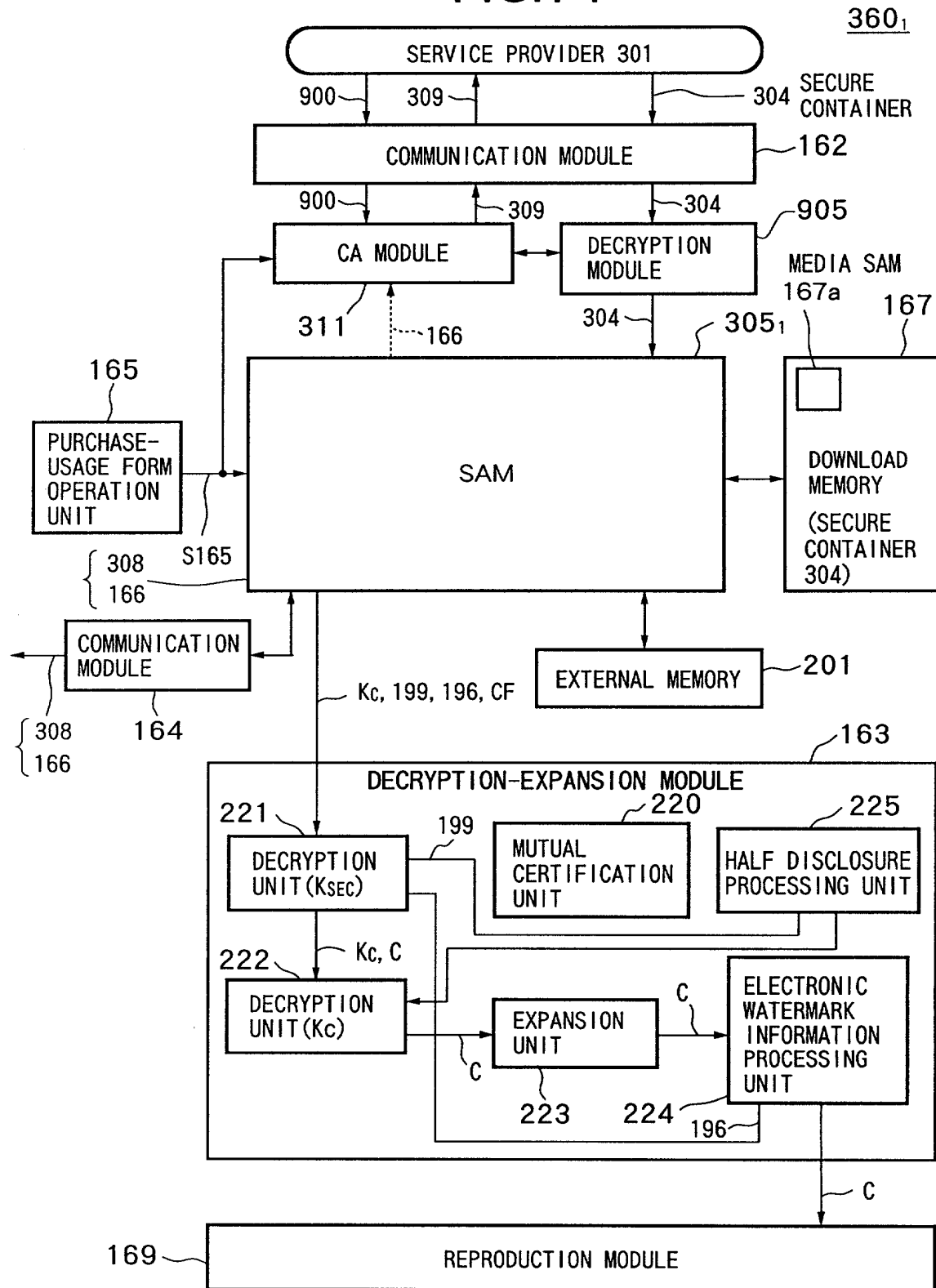


FIG. 75

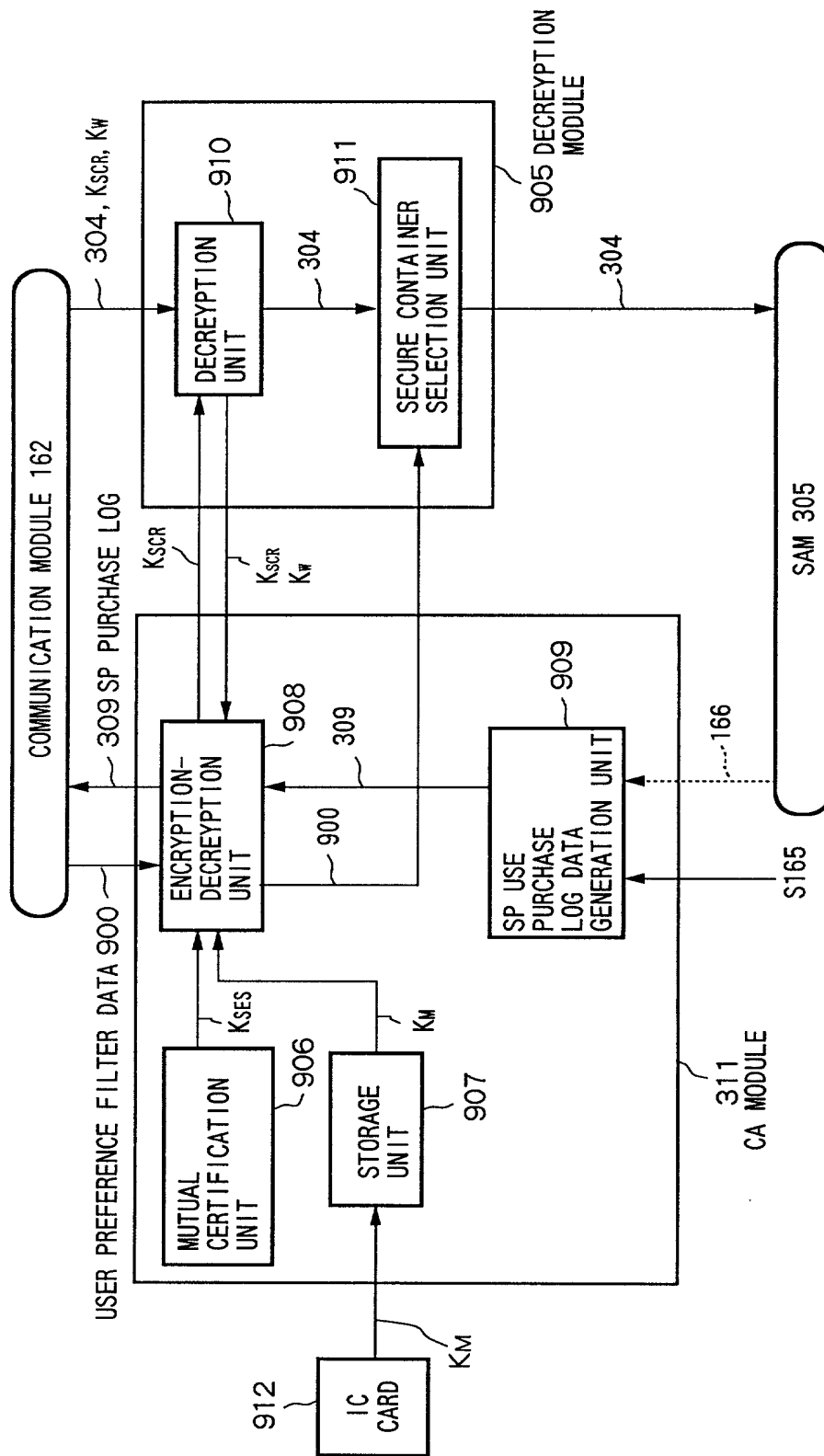
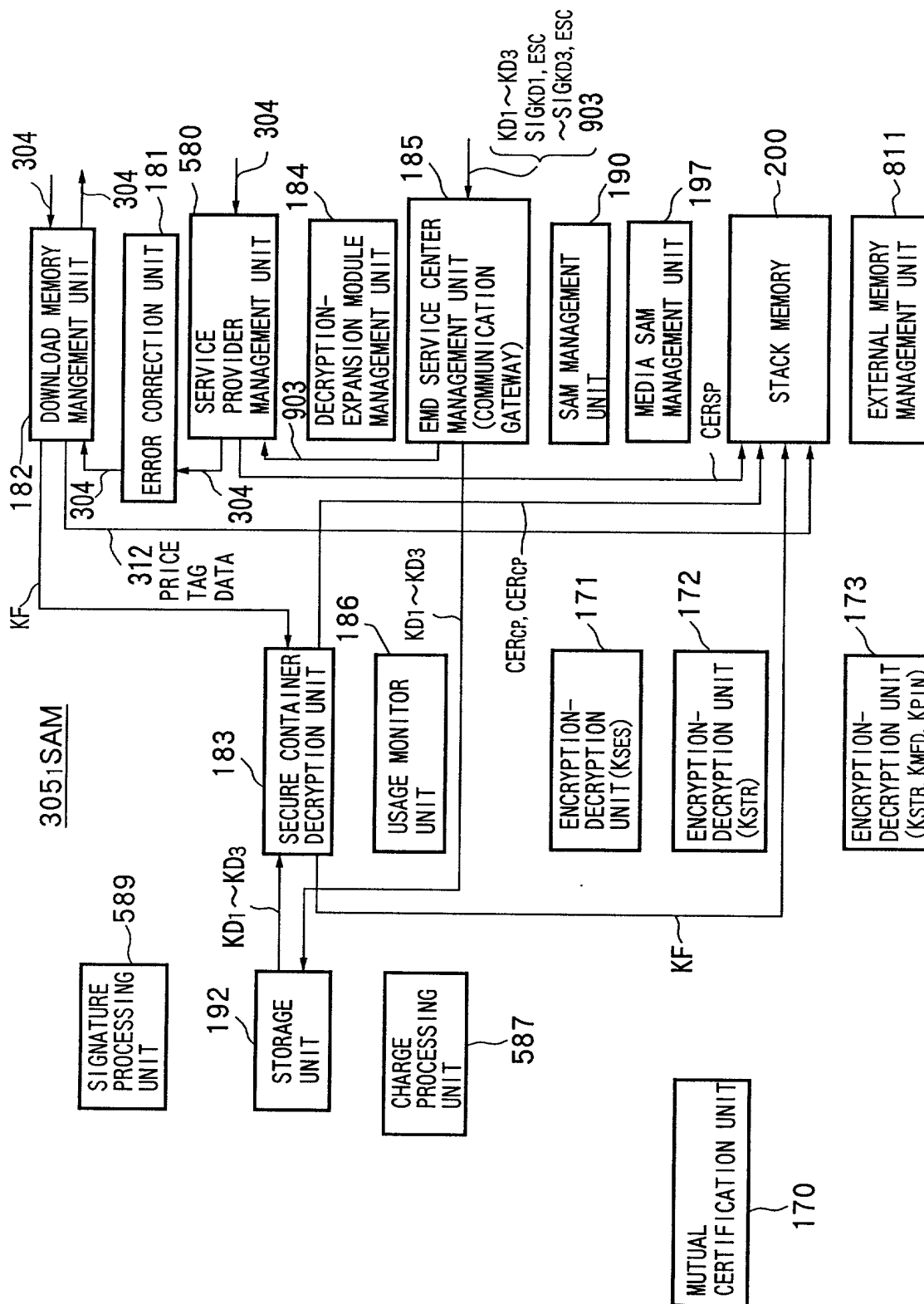


FIG. 76





## FIG.77

STORED DATA OF STACK MEMORY 200

CONTENT KEY DATA  $K_c$

USAGE CONTROL POLICY DATA(UCP) 106

LOCK KEY DATA  $K_{Loc}$  OF NOVOLATILE MEMORY 201

PUBLIC KEY CERTIFICATE DATA  $CER_{CP}$  OF CONTENT PROVIDER 301

PUBLIC KEY CERTIFICATE DATA  $CER_{SP}$  OF SERVICE PROVIDER 301

USAGE CONTROL STATUS DATA(UCS) 166

SAM PROGRAM DOWNLOAD CONTAINERS  $SD_1 \sim SDC_3$

PRICE TAG DATA 312

**FIG. 78**

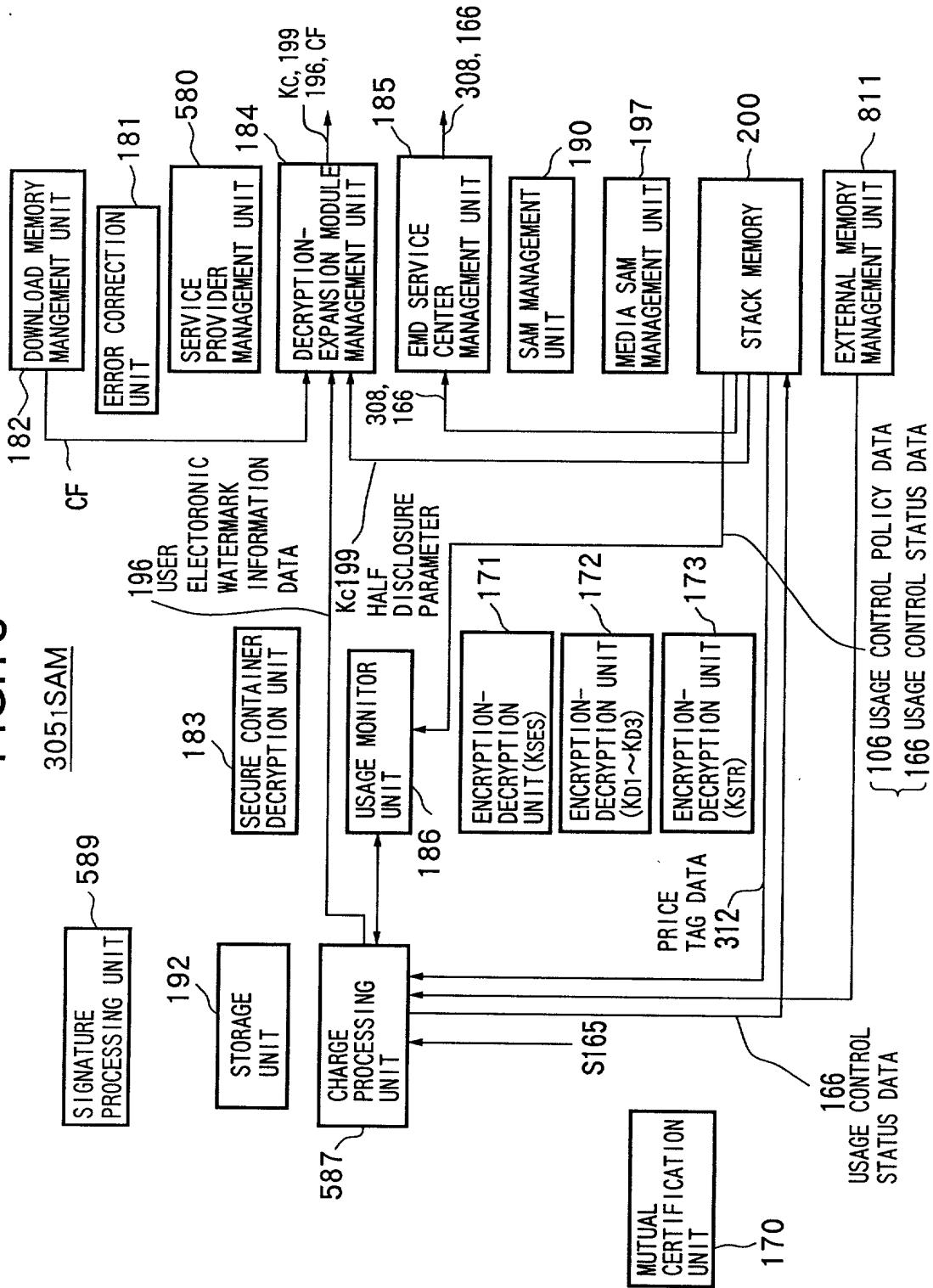


FIG.79

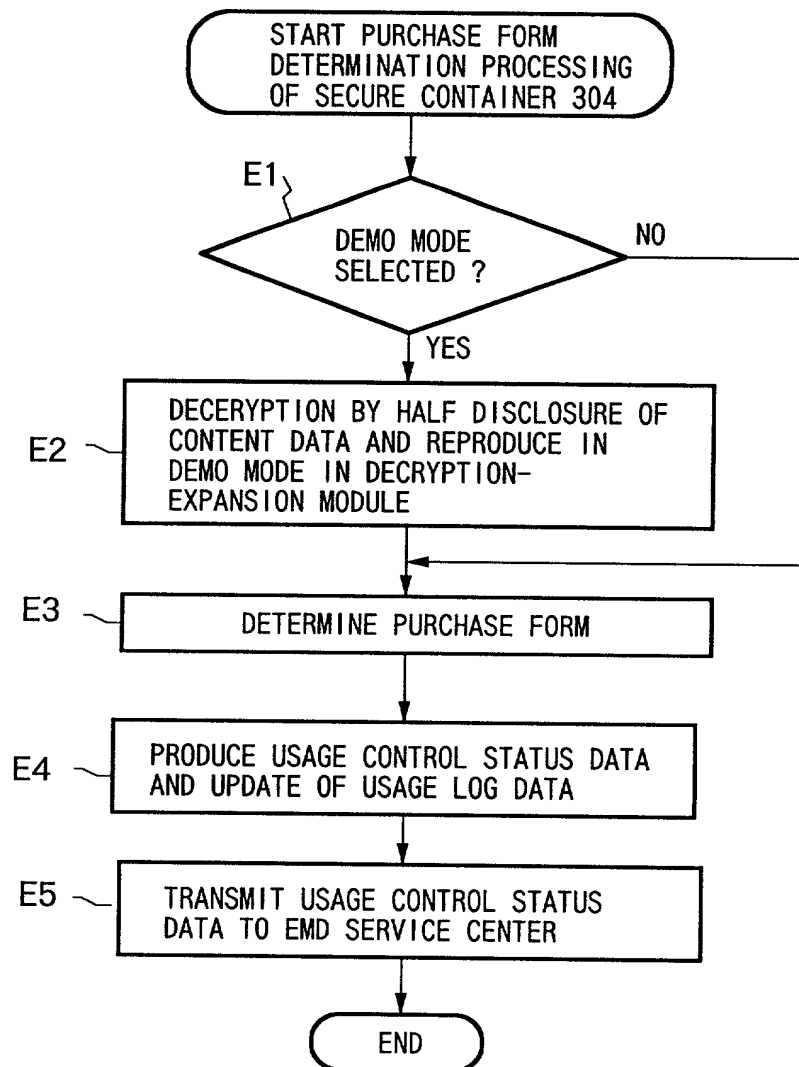
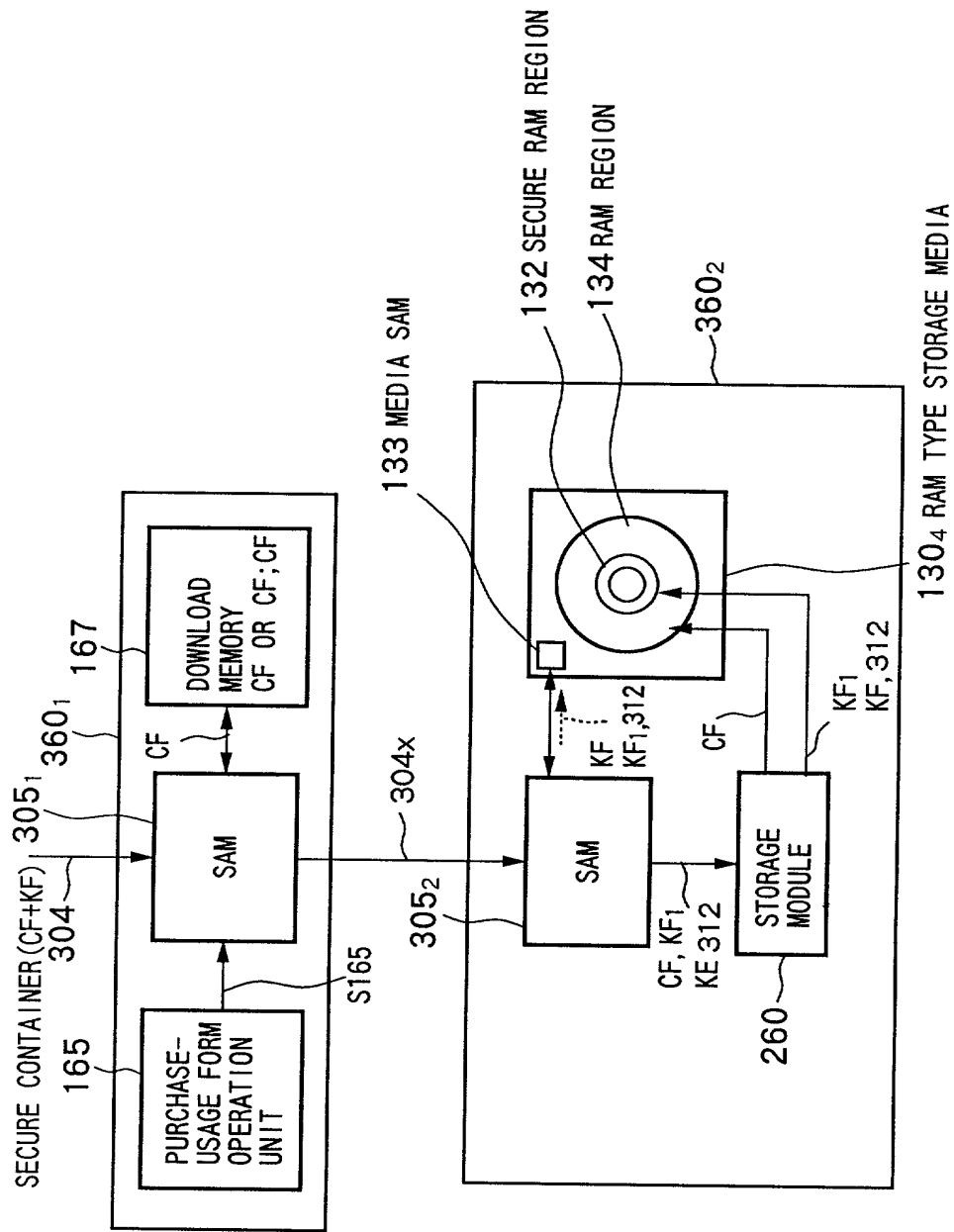


FIG. 80



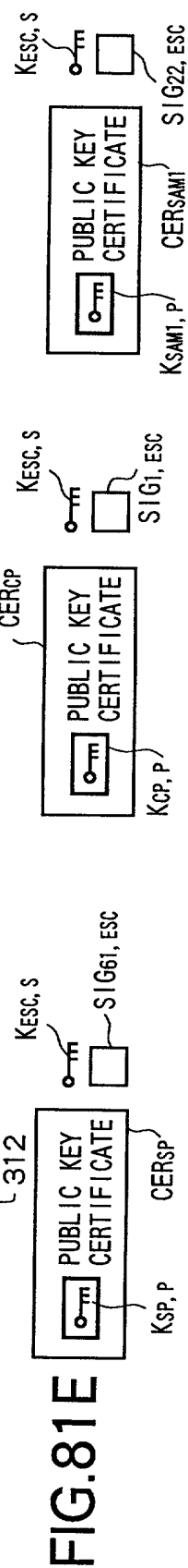
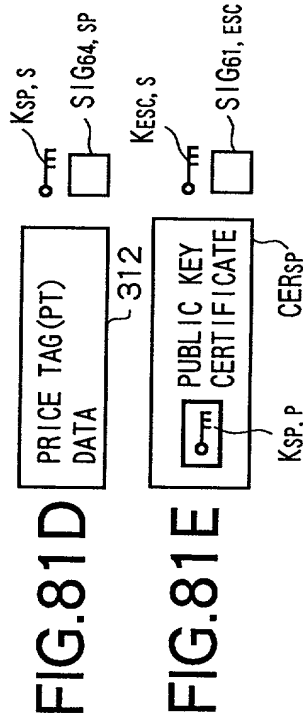
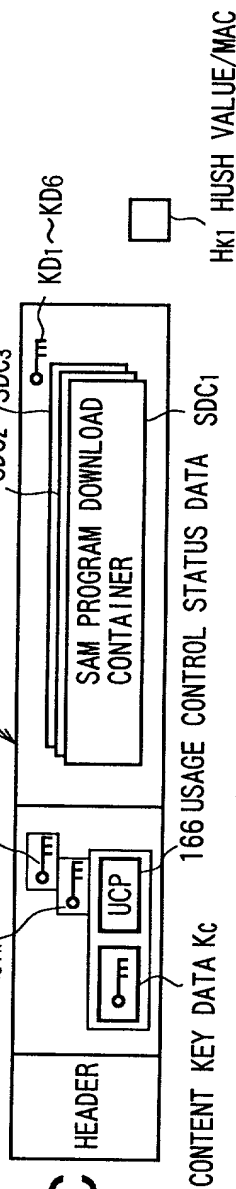
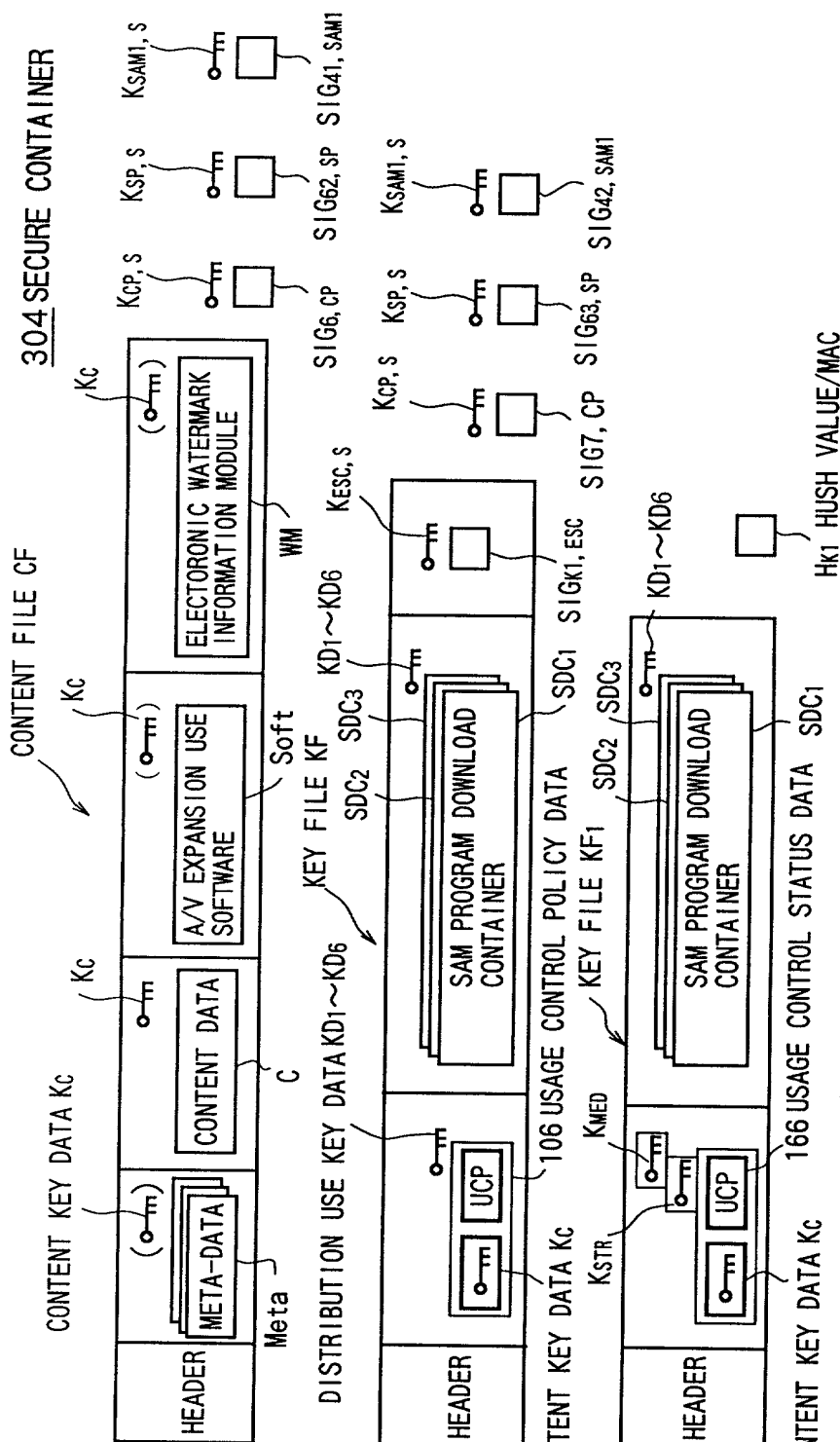


FIG. 82

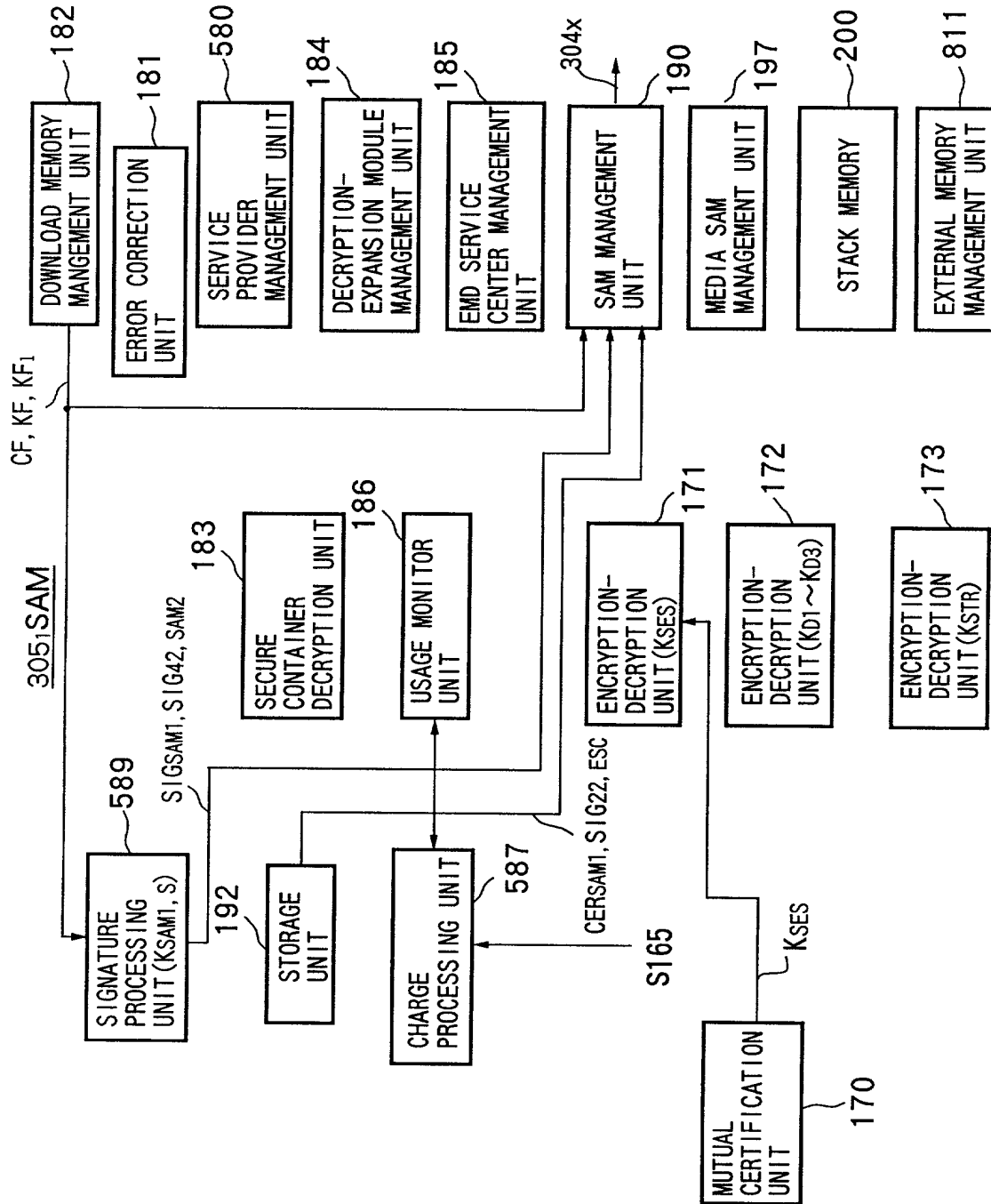


FIG. 83

305<sub>2</sub>SAM

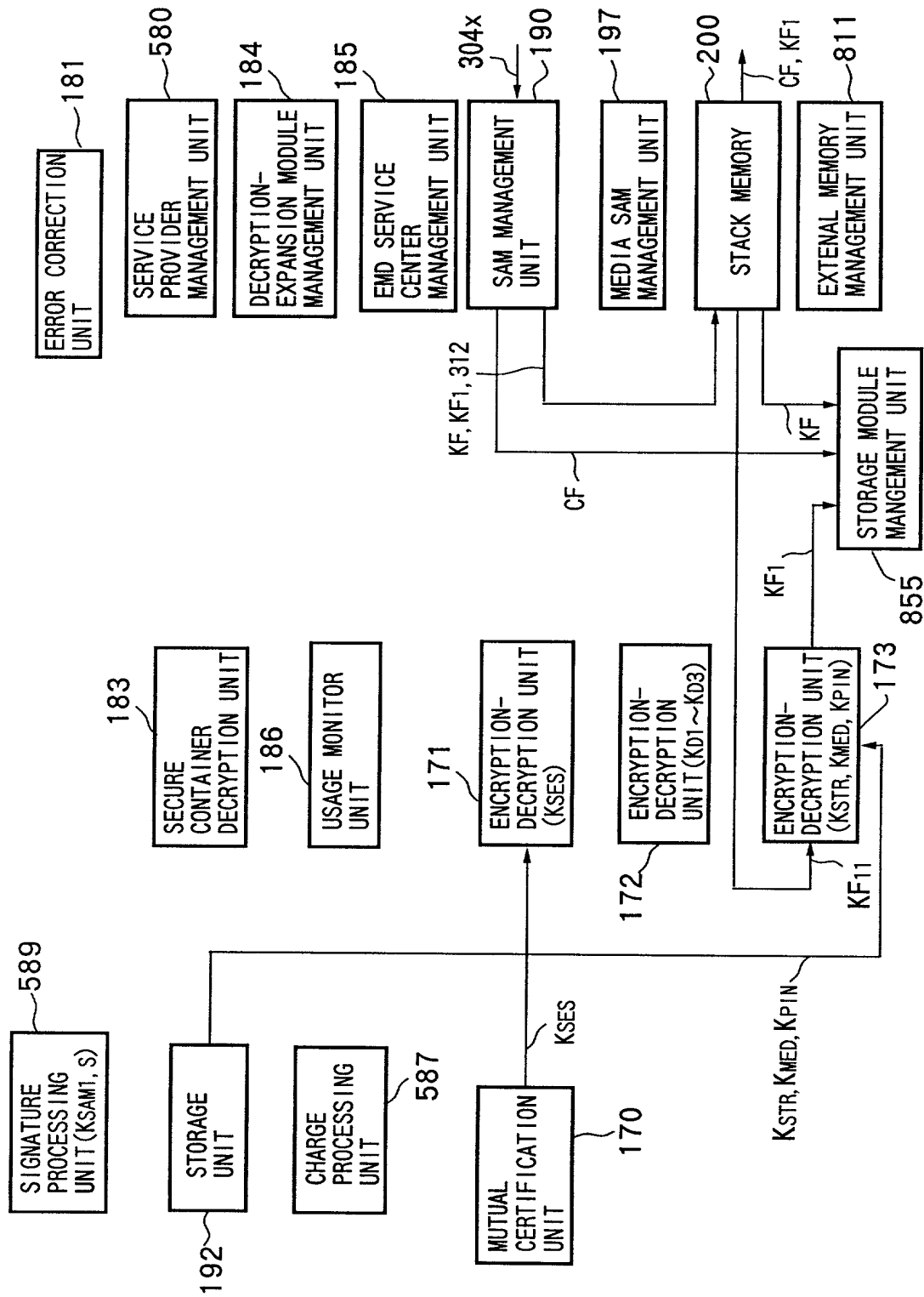


FIG.84

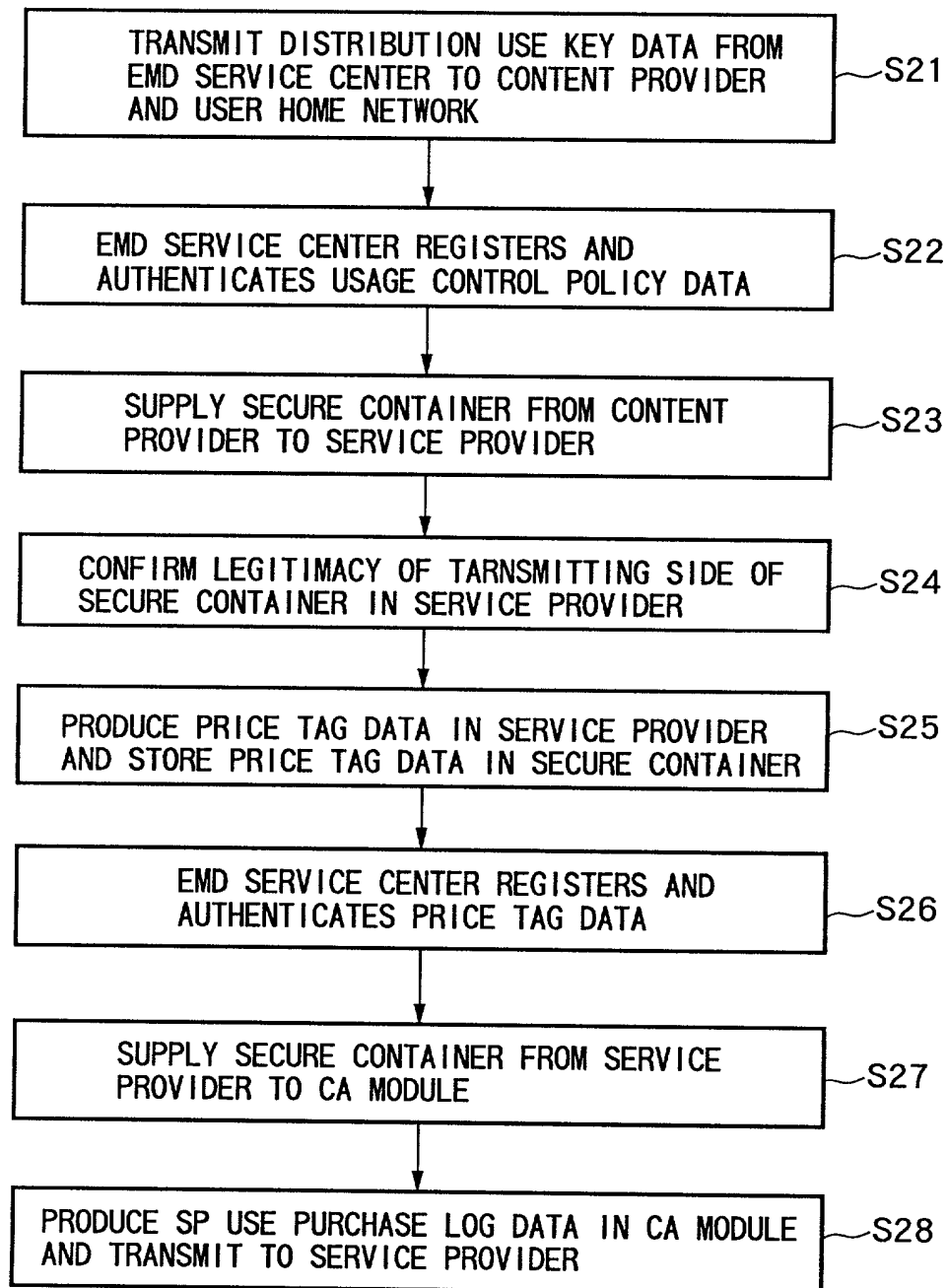




FIG.85

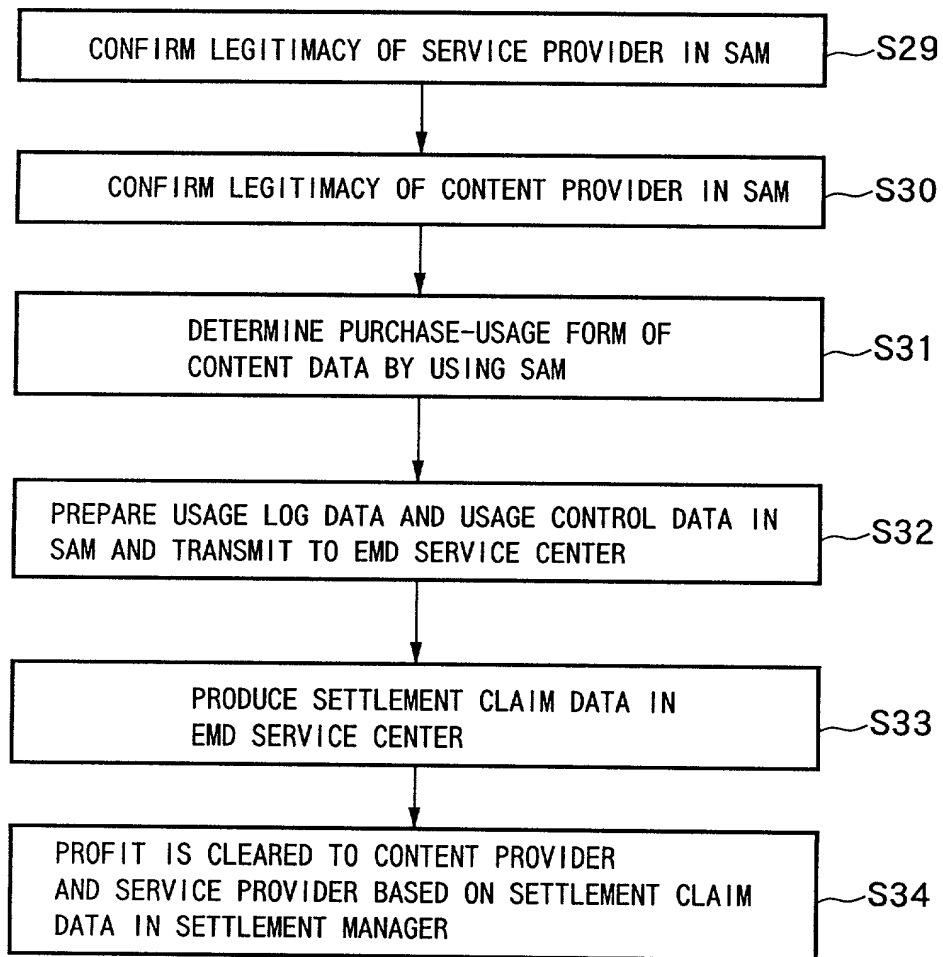
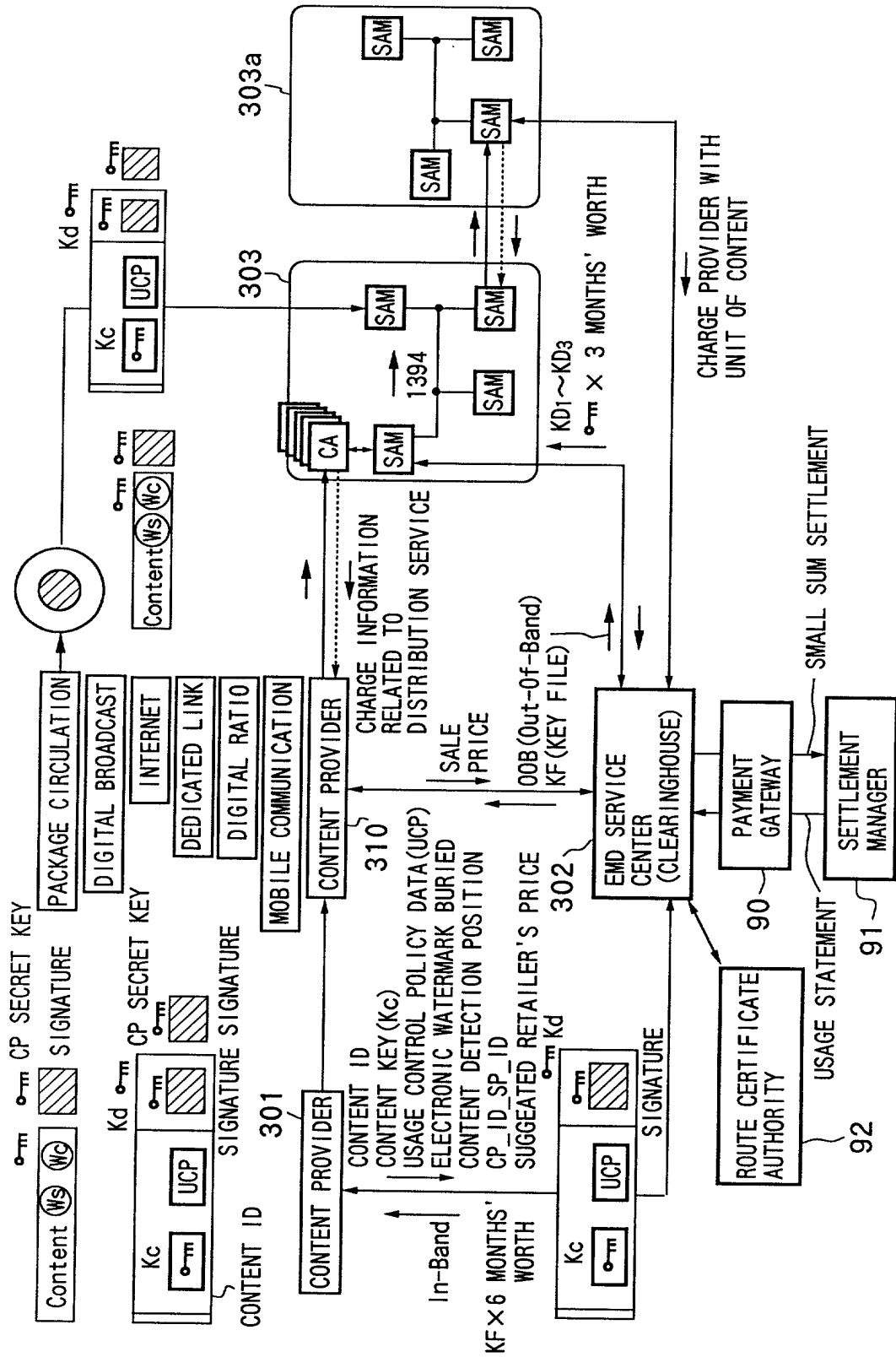
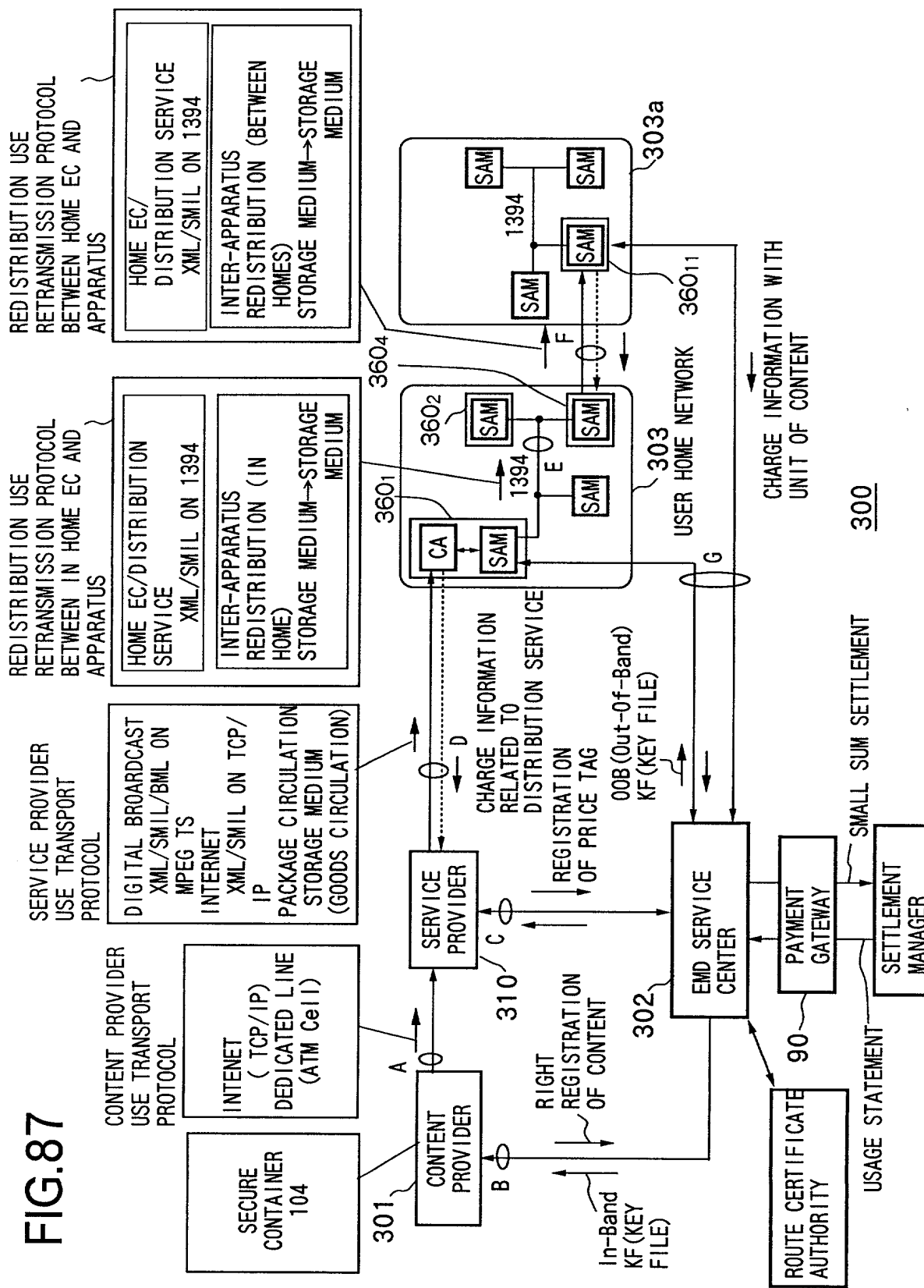


FIG. 86





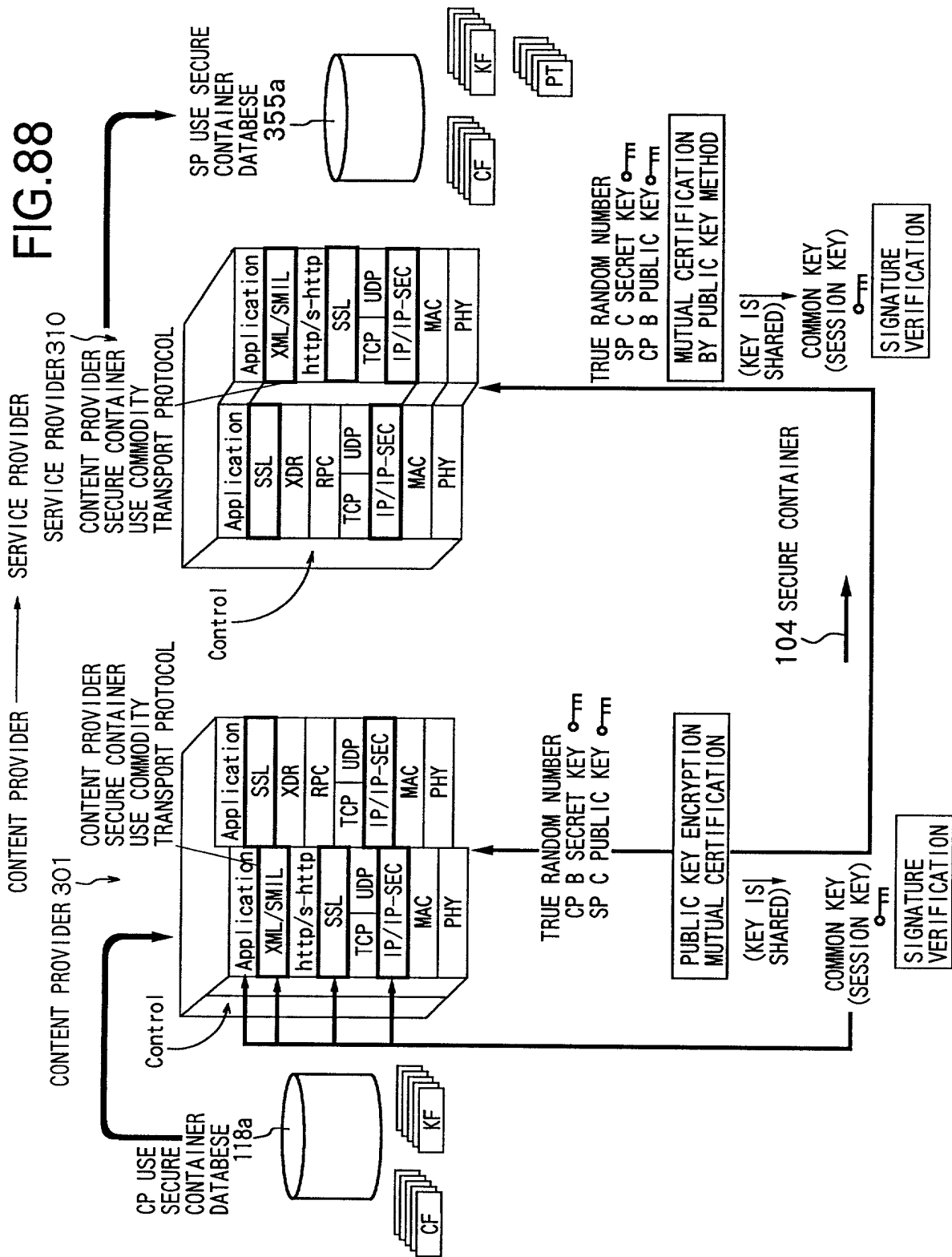


FIG.89

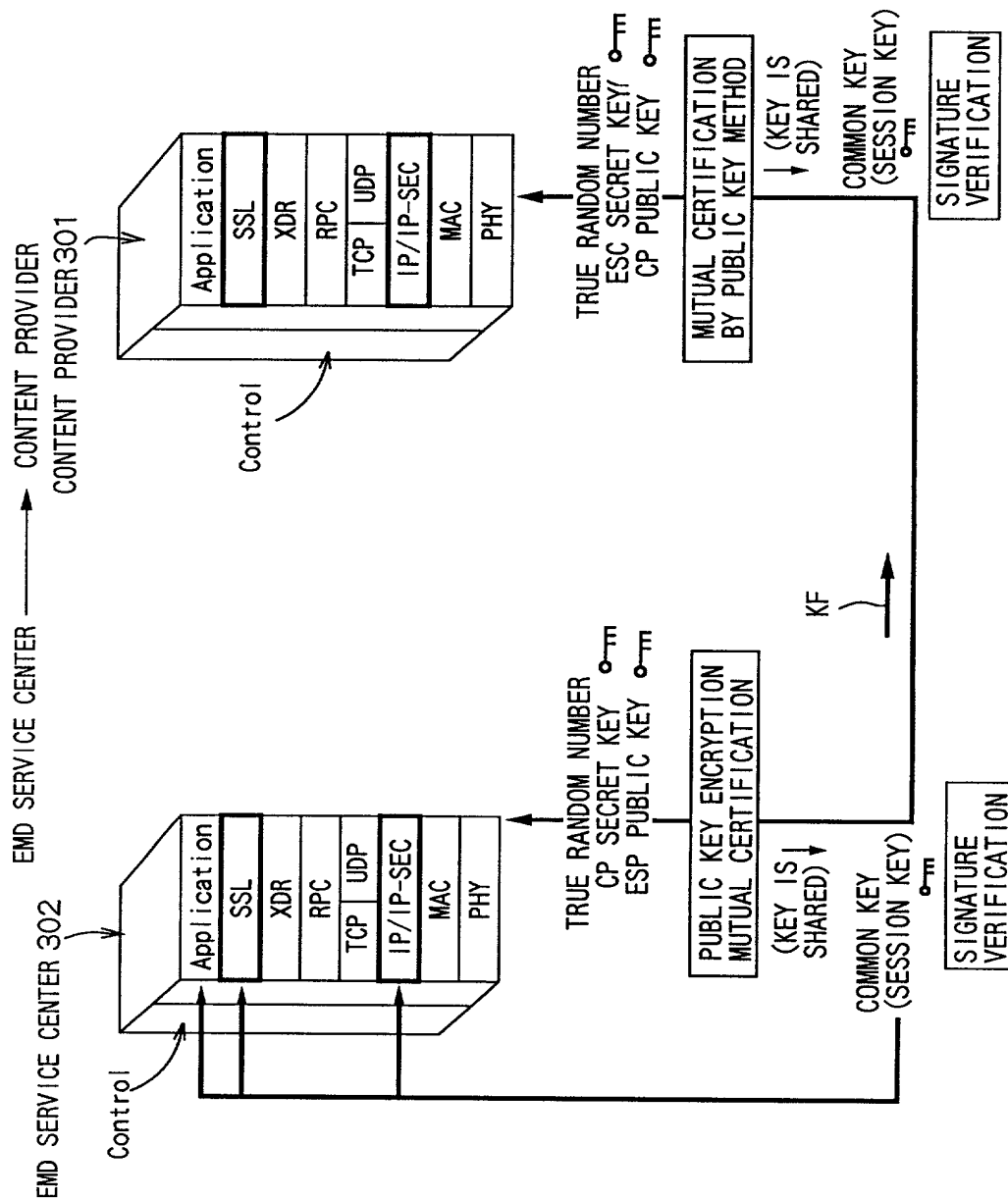


FIG. 90

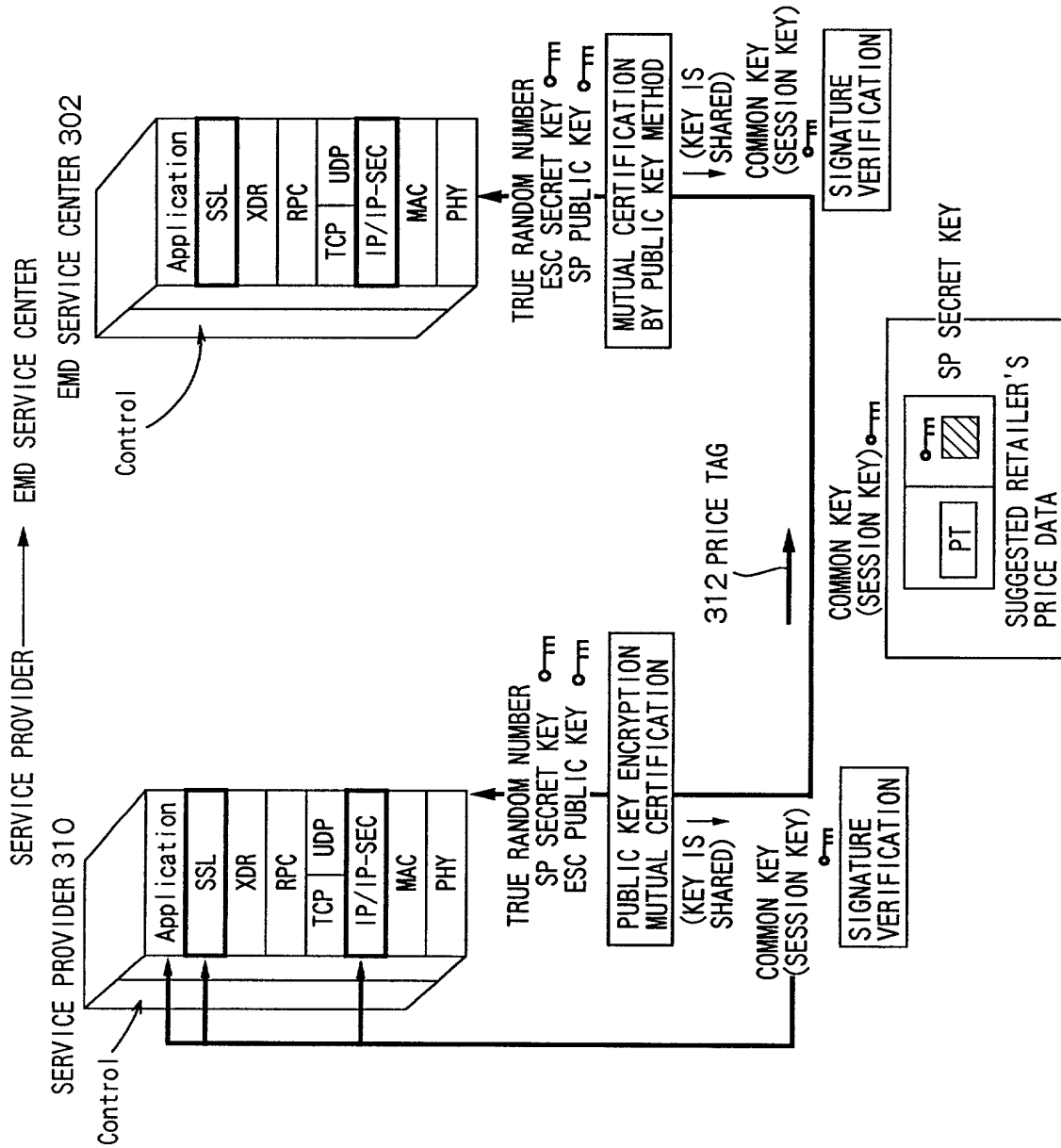


FIG. 91

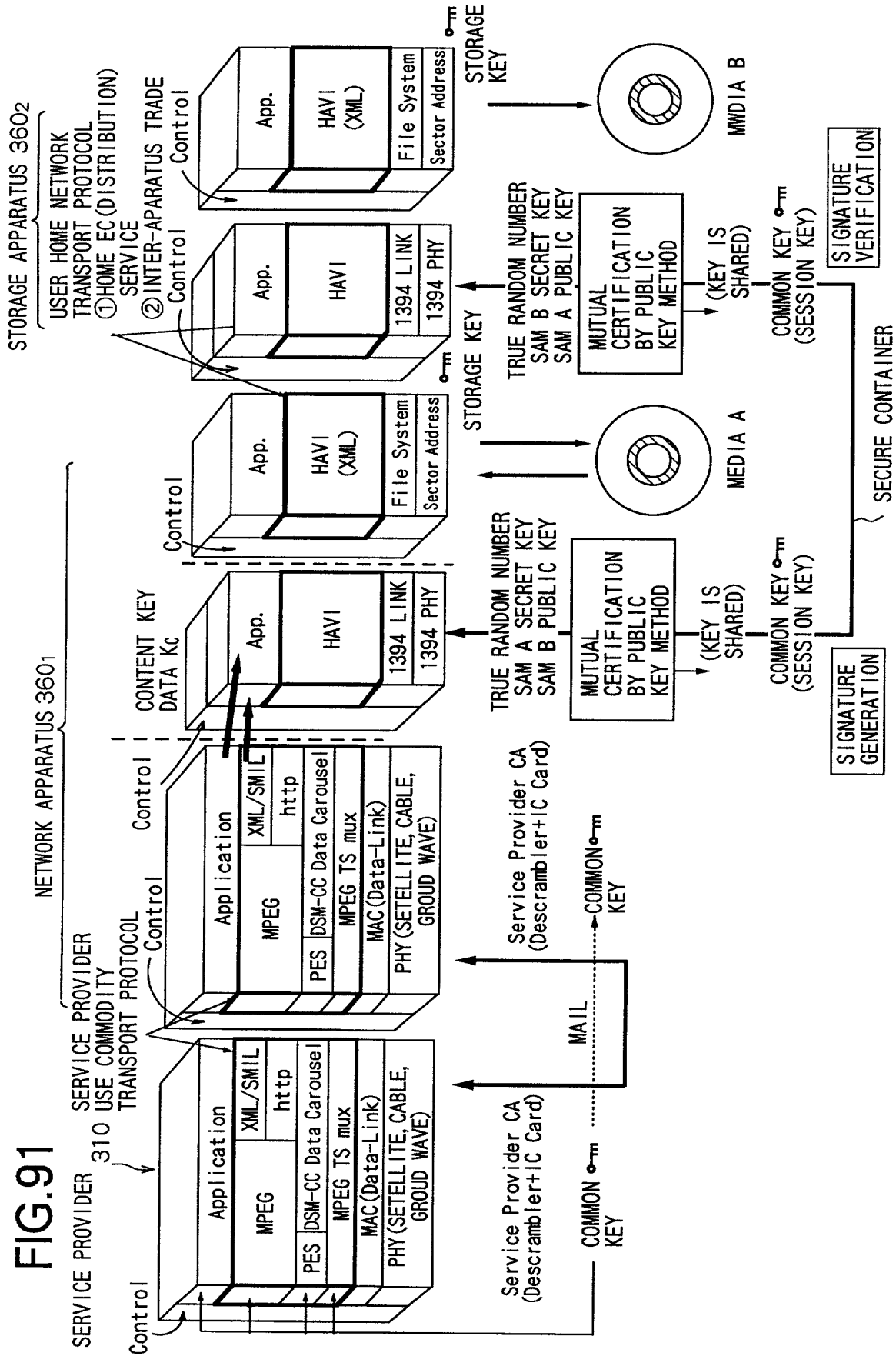


FIG. 92

INCREMENT OF SECURE CONTAINER TO PROTOCOL CLASS WHERE  
XML/SMIL/BML IS USED IN DATA BROADCAST METHOD OF DIGITAL BROADCAST

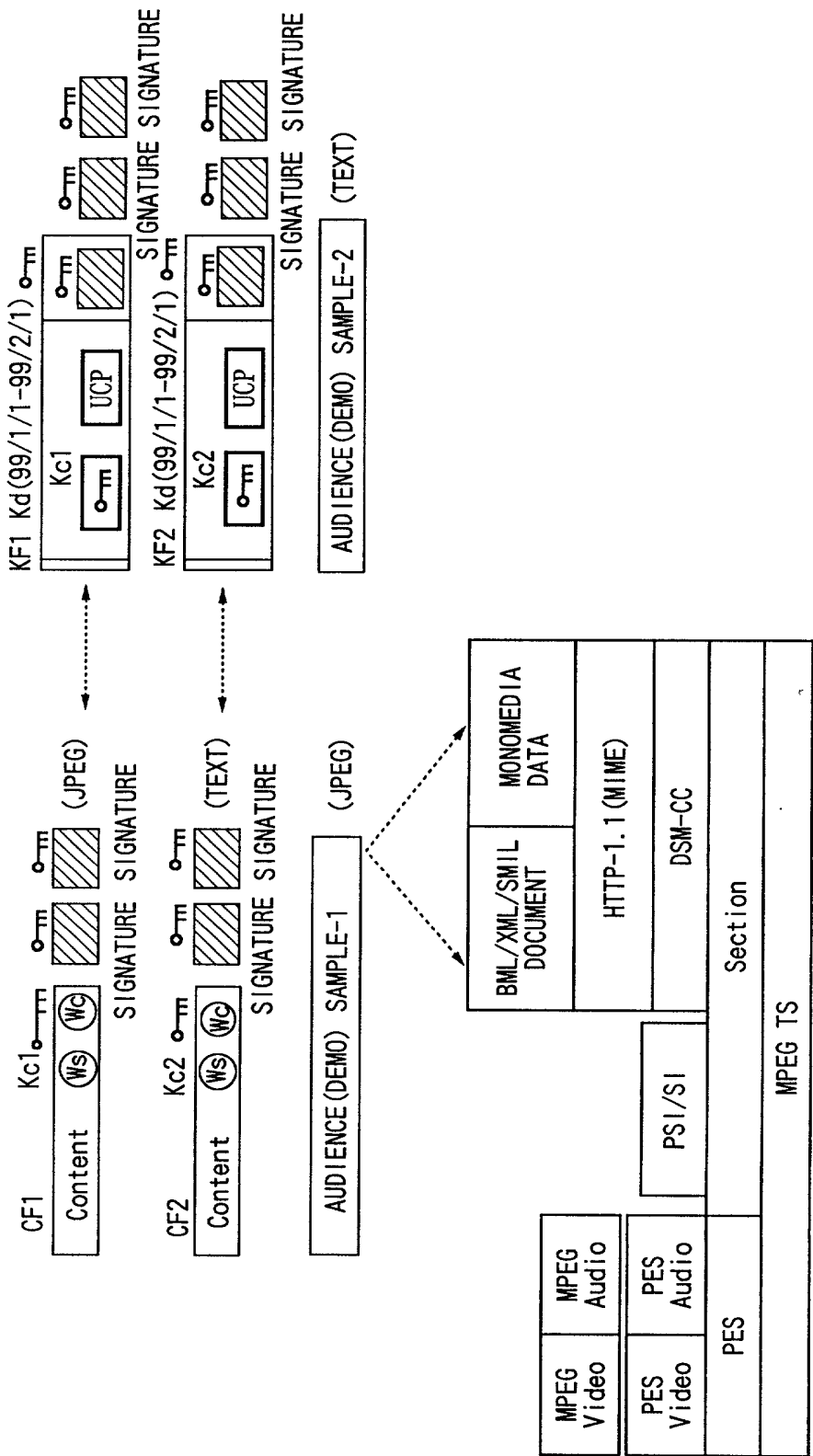




FIG.93

INCREMENT OF SECURE CONTAINER TO PROTOCOL CLASS WHERE  
MHEG IS USED IN DATA BROADCAST METHOD OF DIGITAL BROADCAST

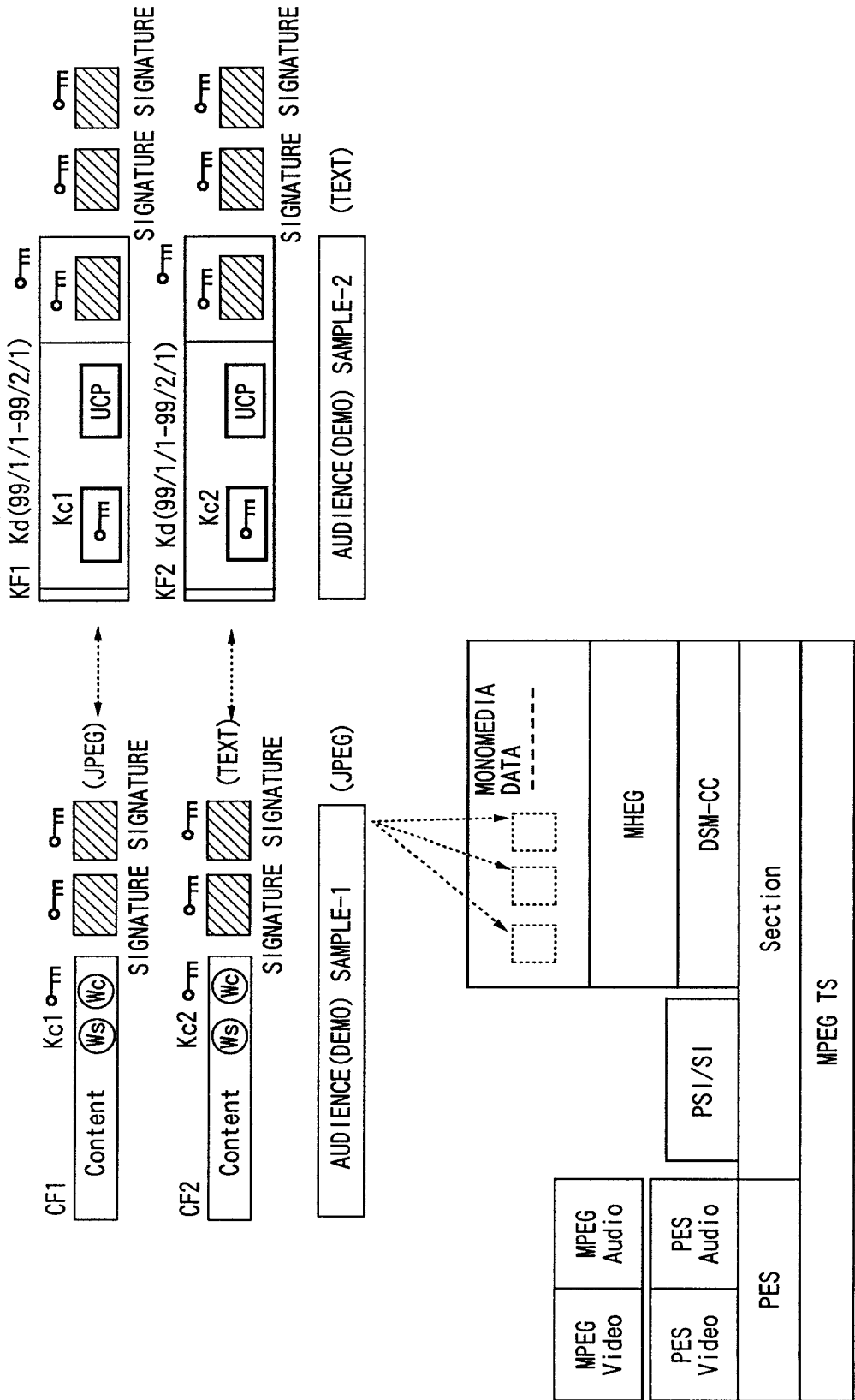
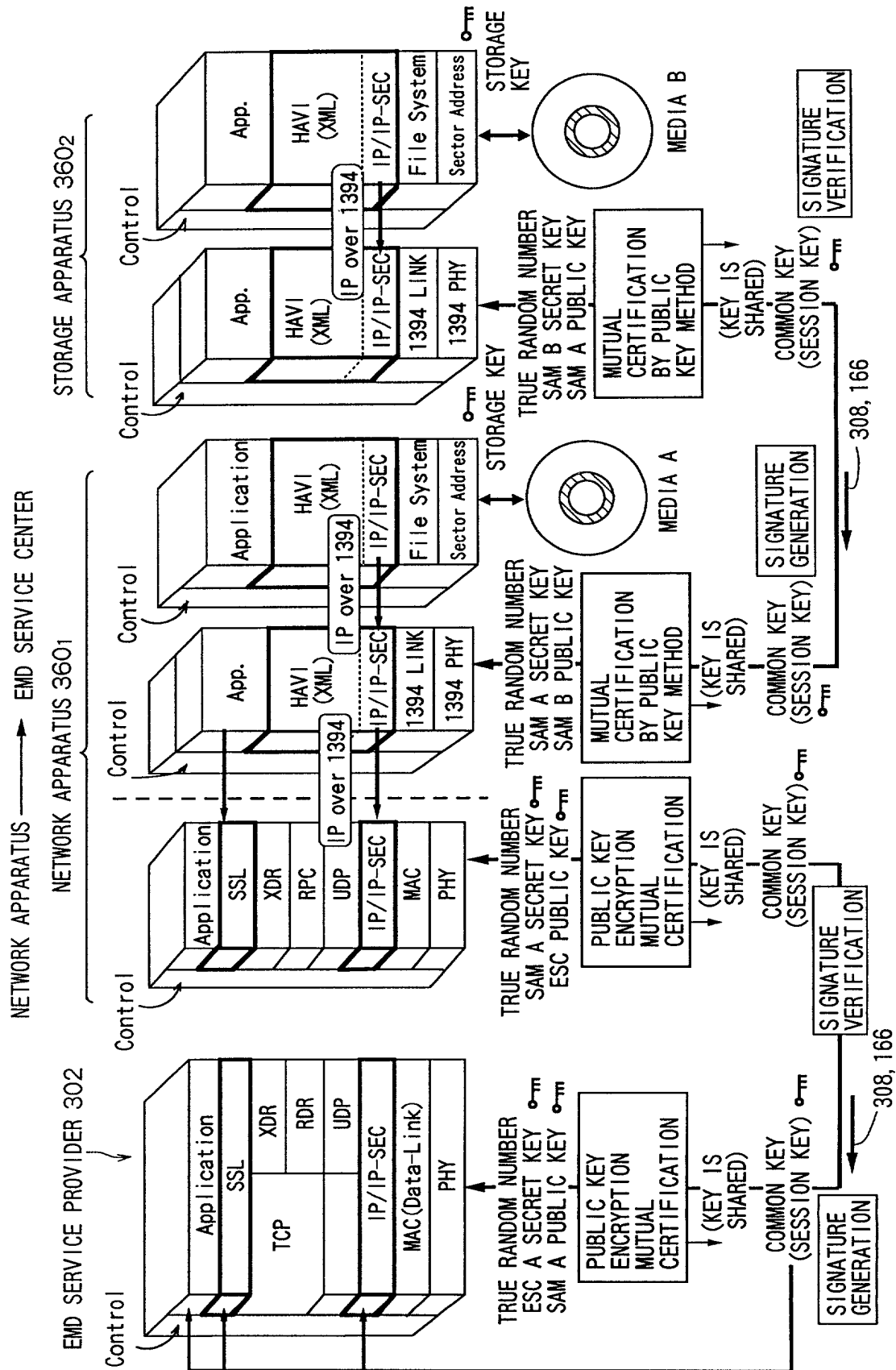




FIG. 95



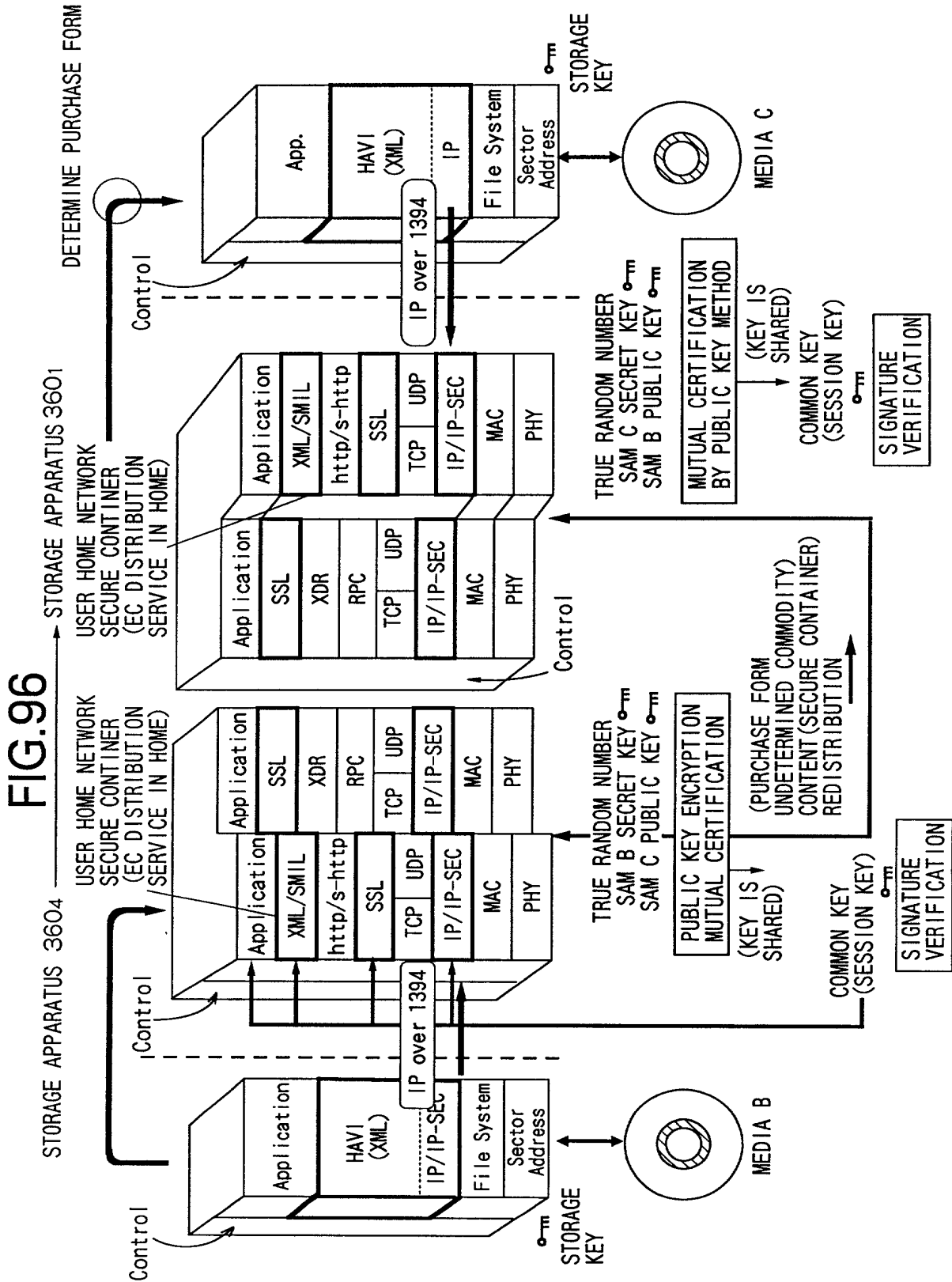
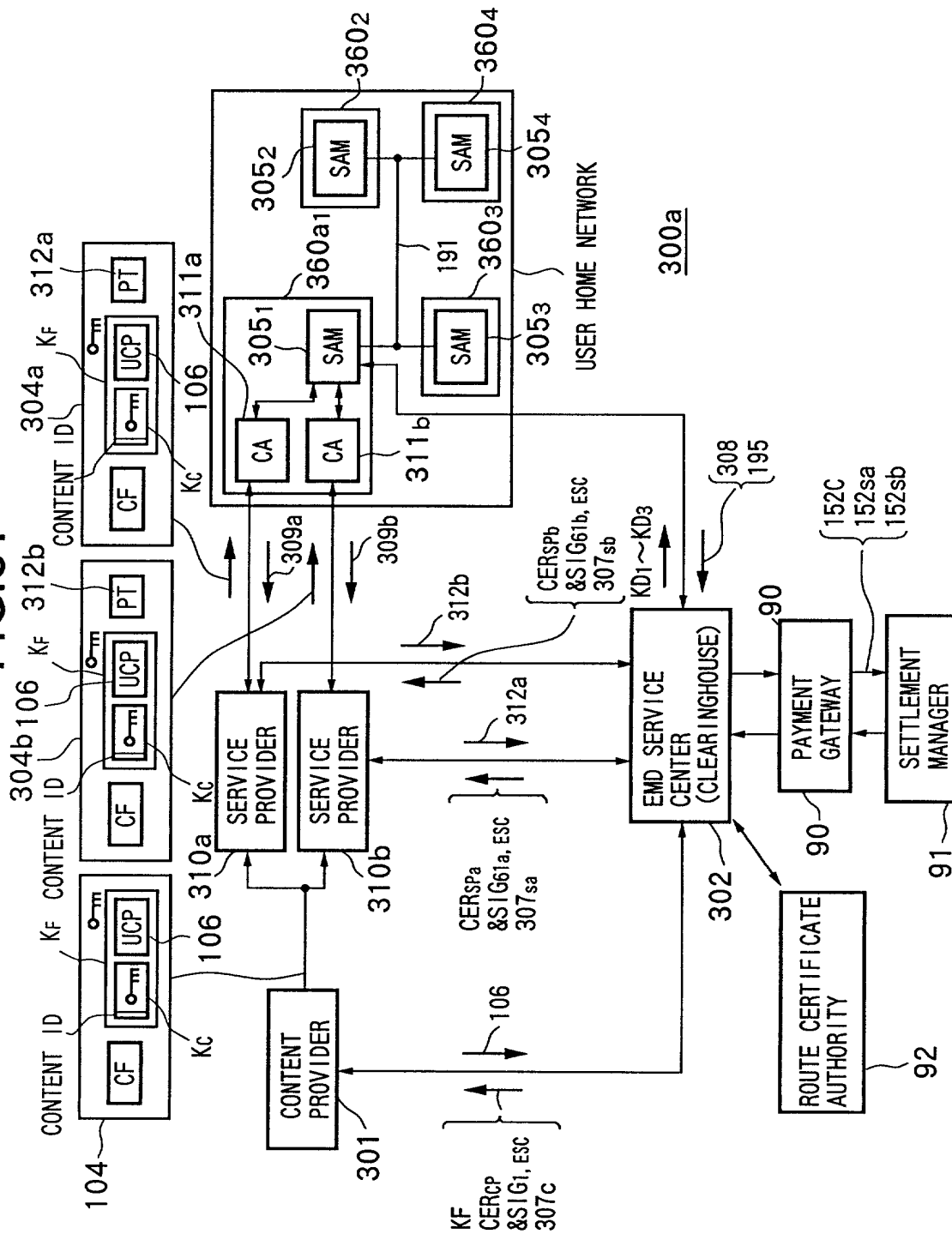


FIG. 97



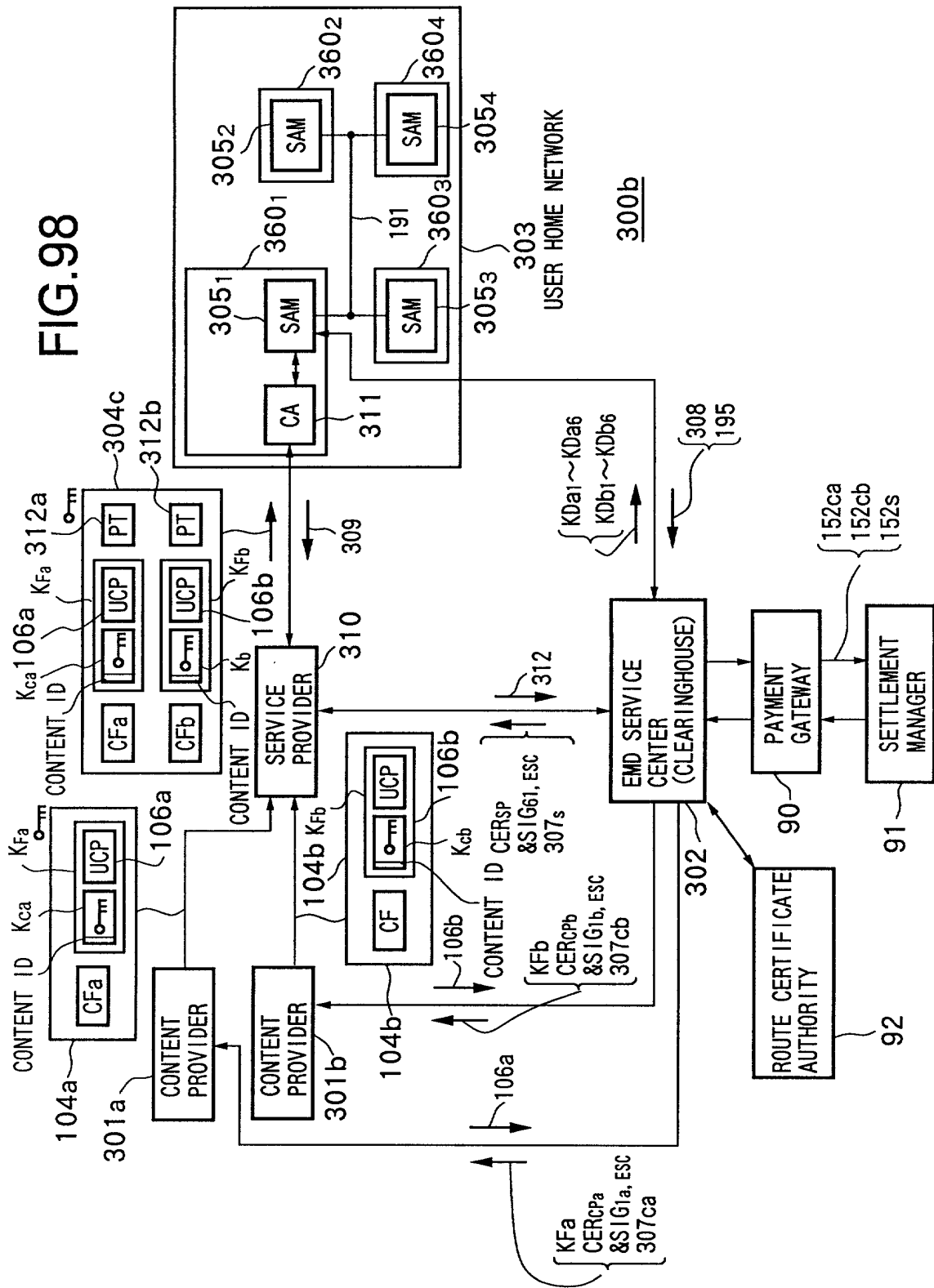


FIG. 99

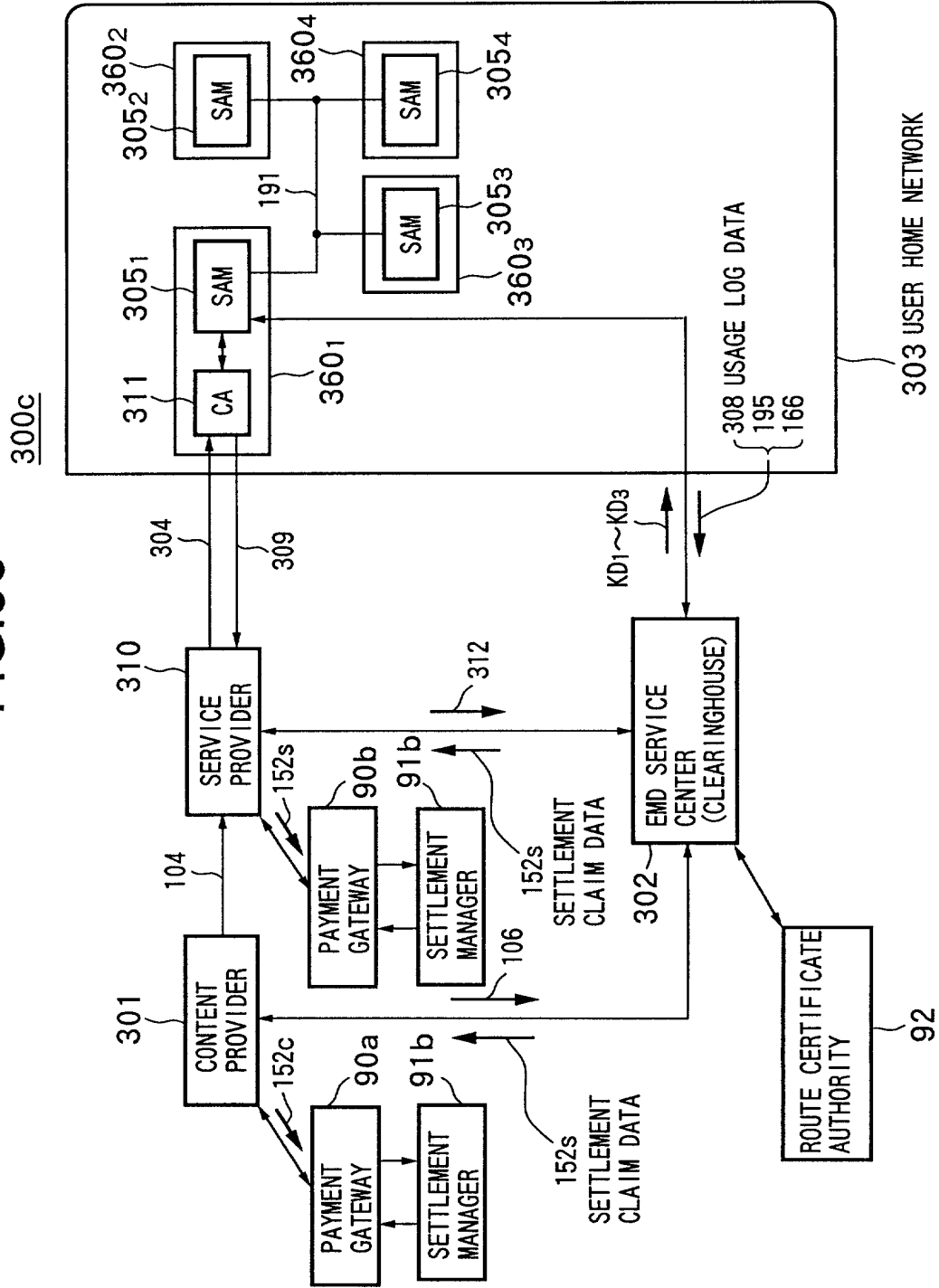
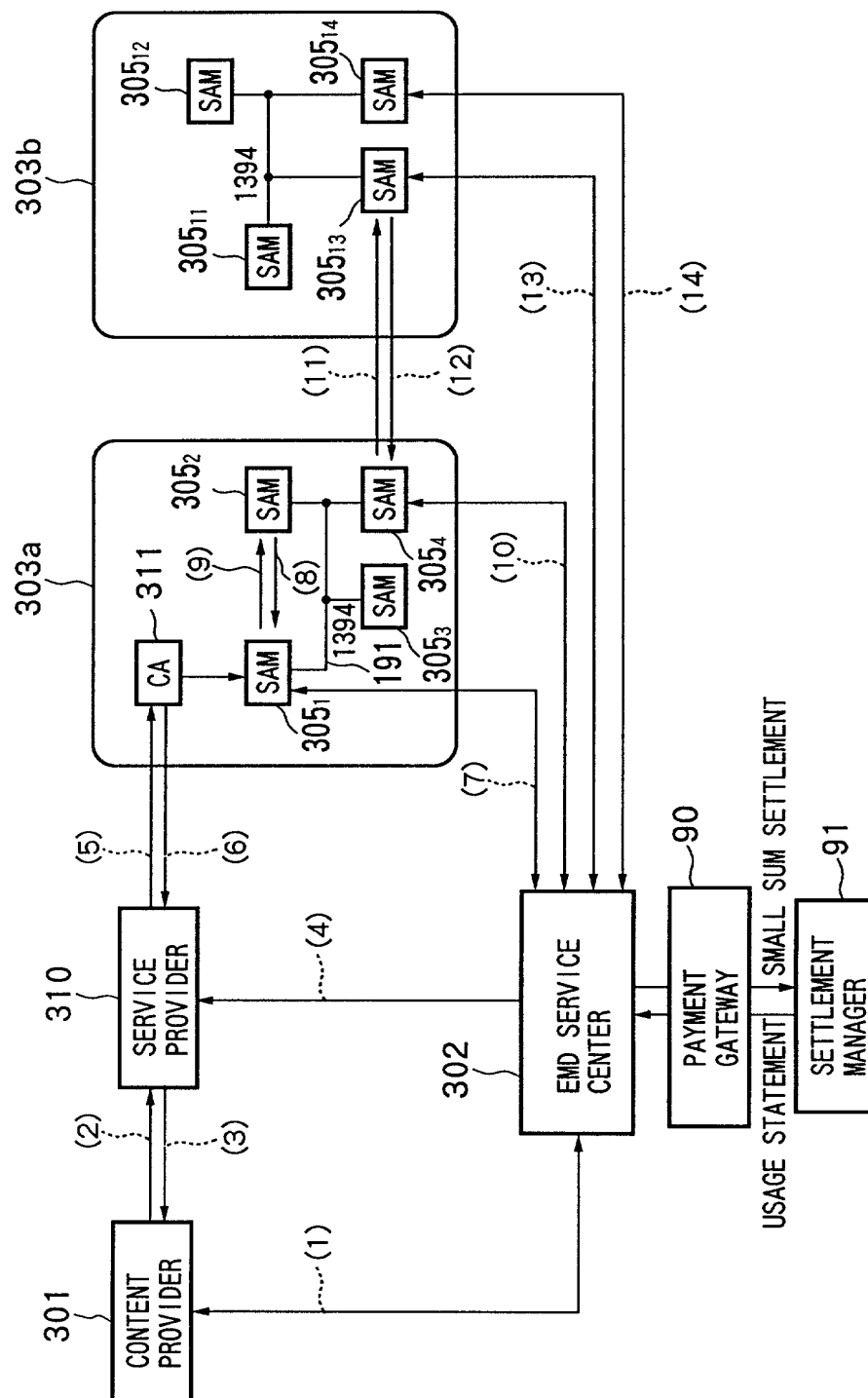






FIG.101



ACQUISITION ROUTE OF PUBLIC KEY CERTIFICATE

FIG. 102

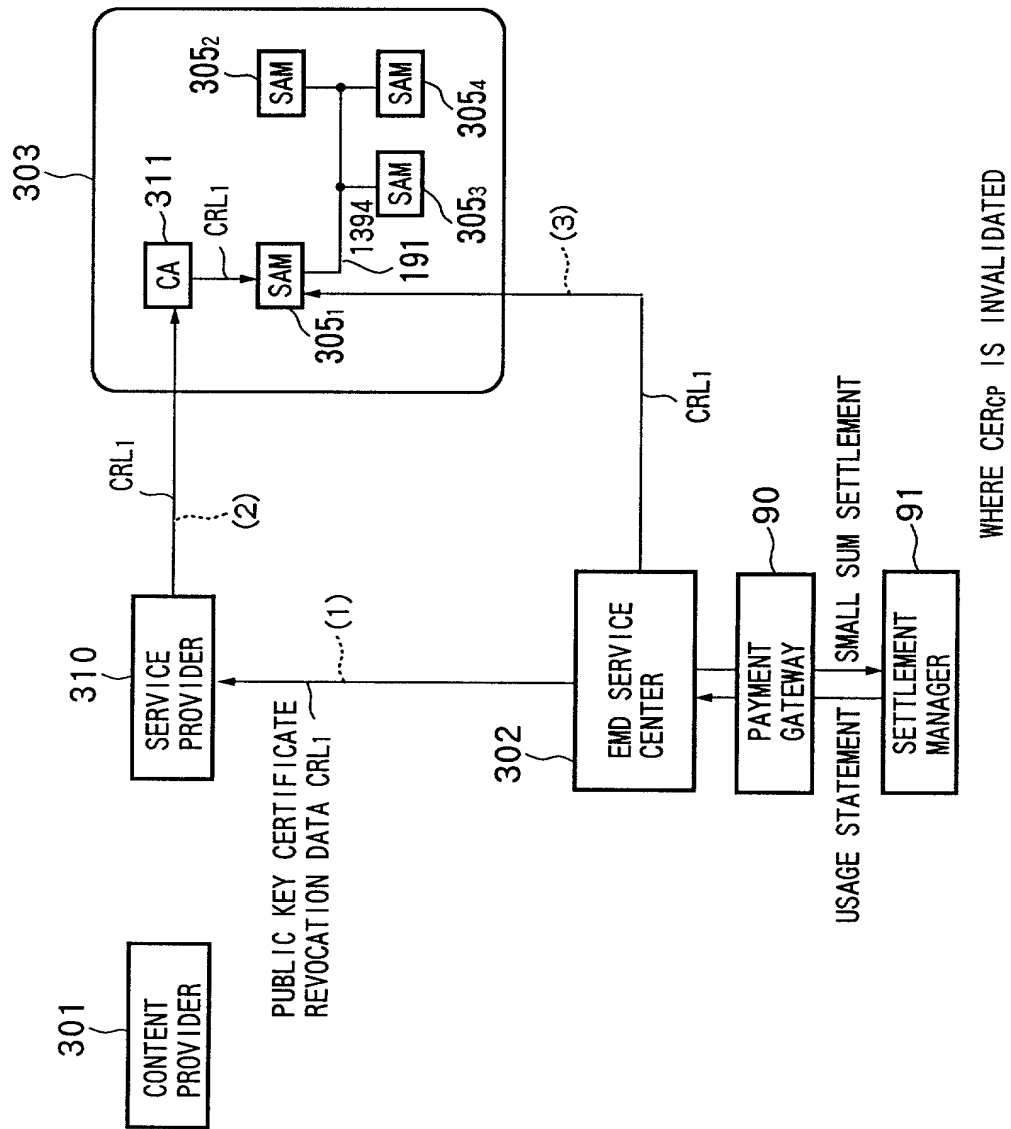


FIG. 103

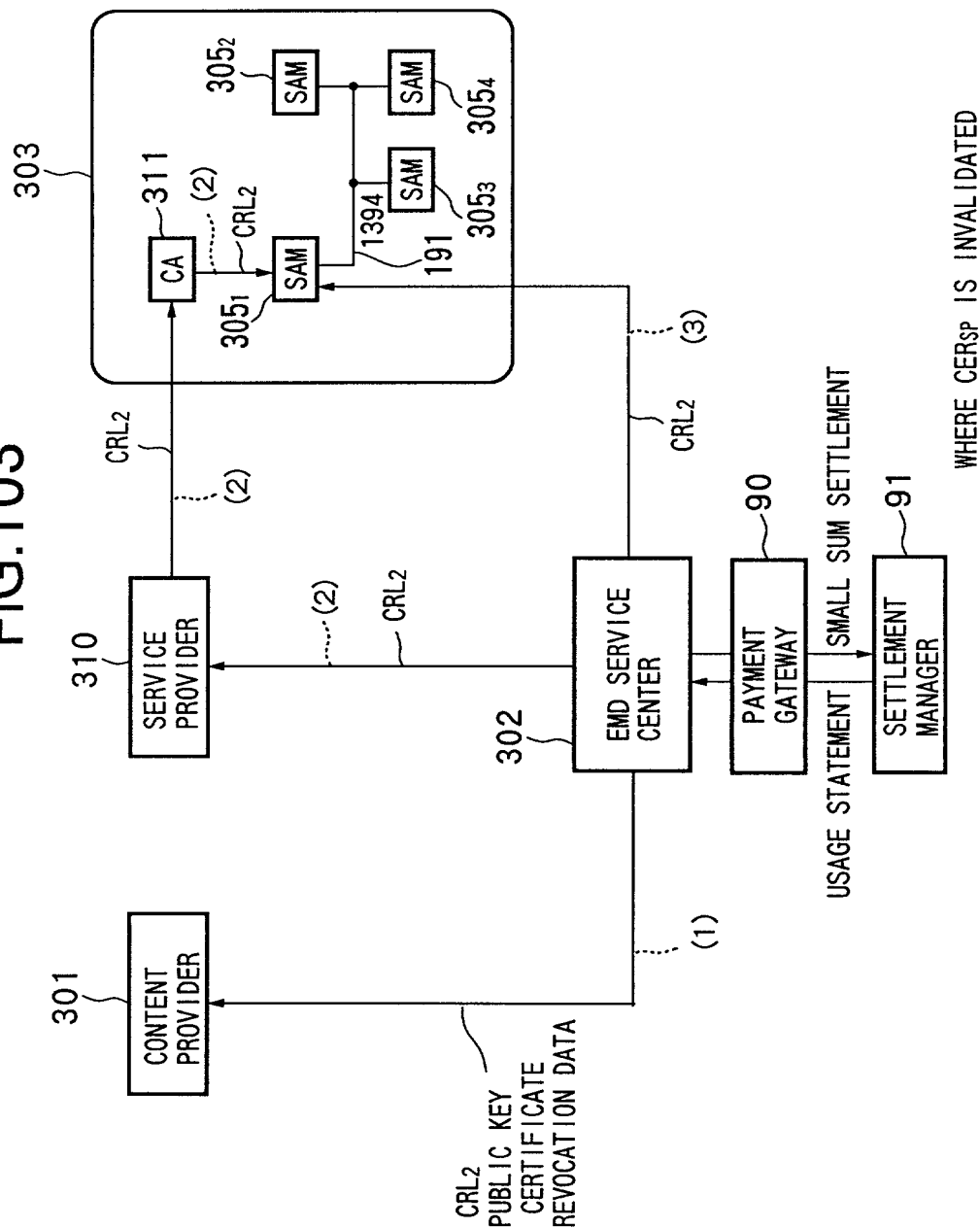
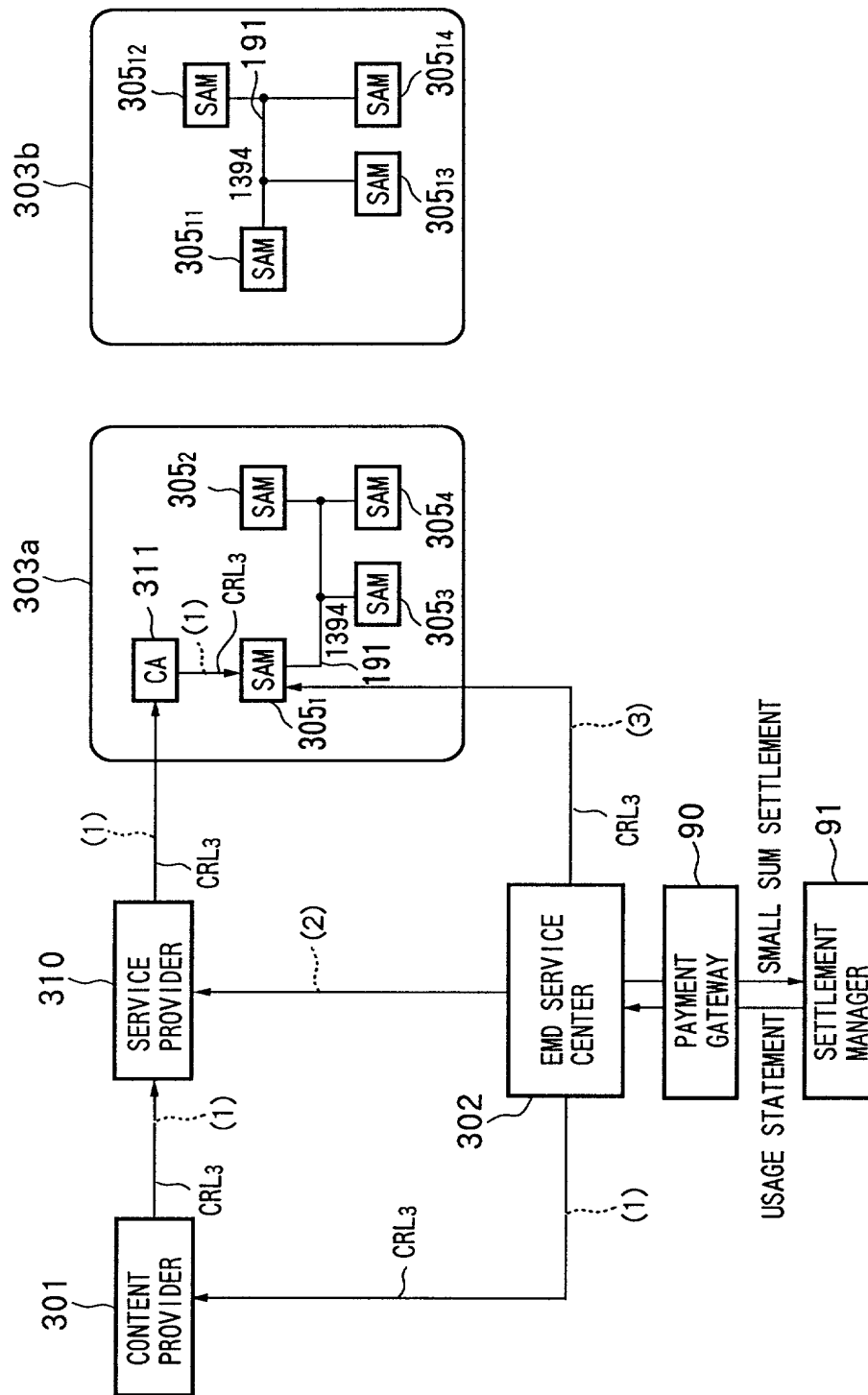
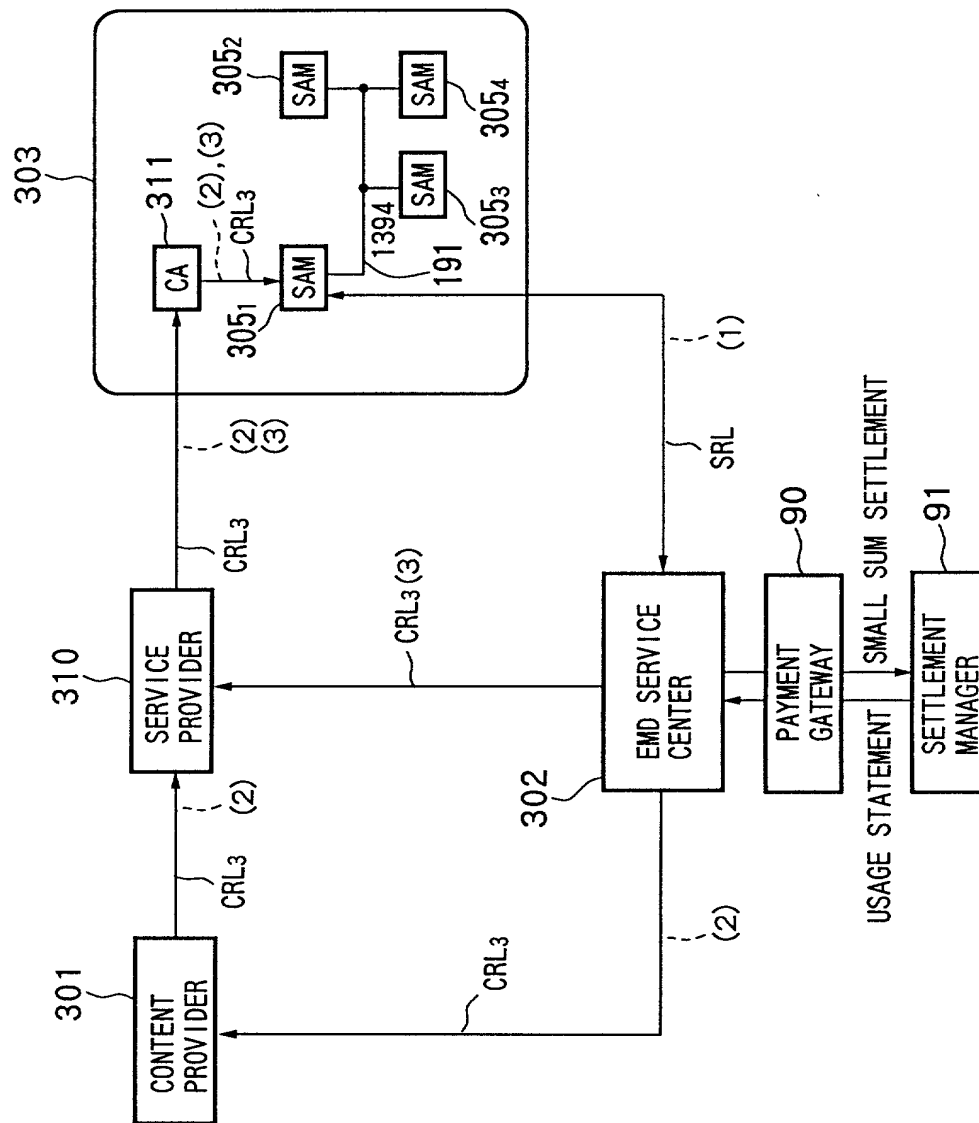


FIG.104

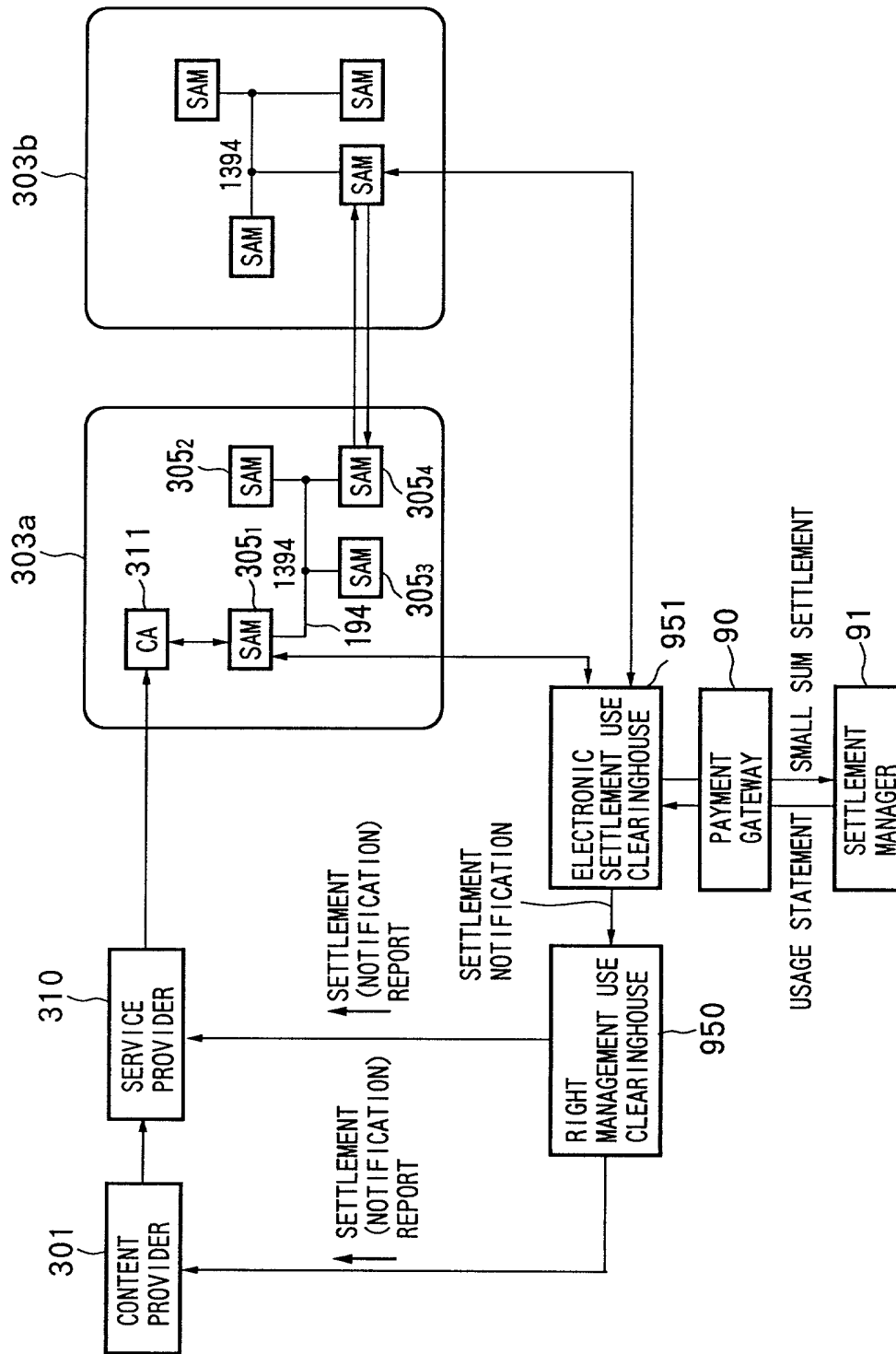


WHERE CERSAM2 IS INVALIDATED

FIG.105



103/143



104/143

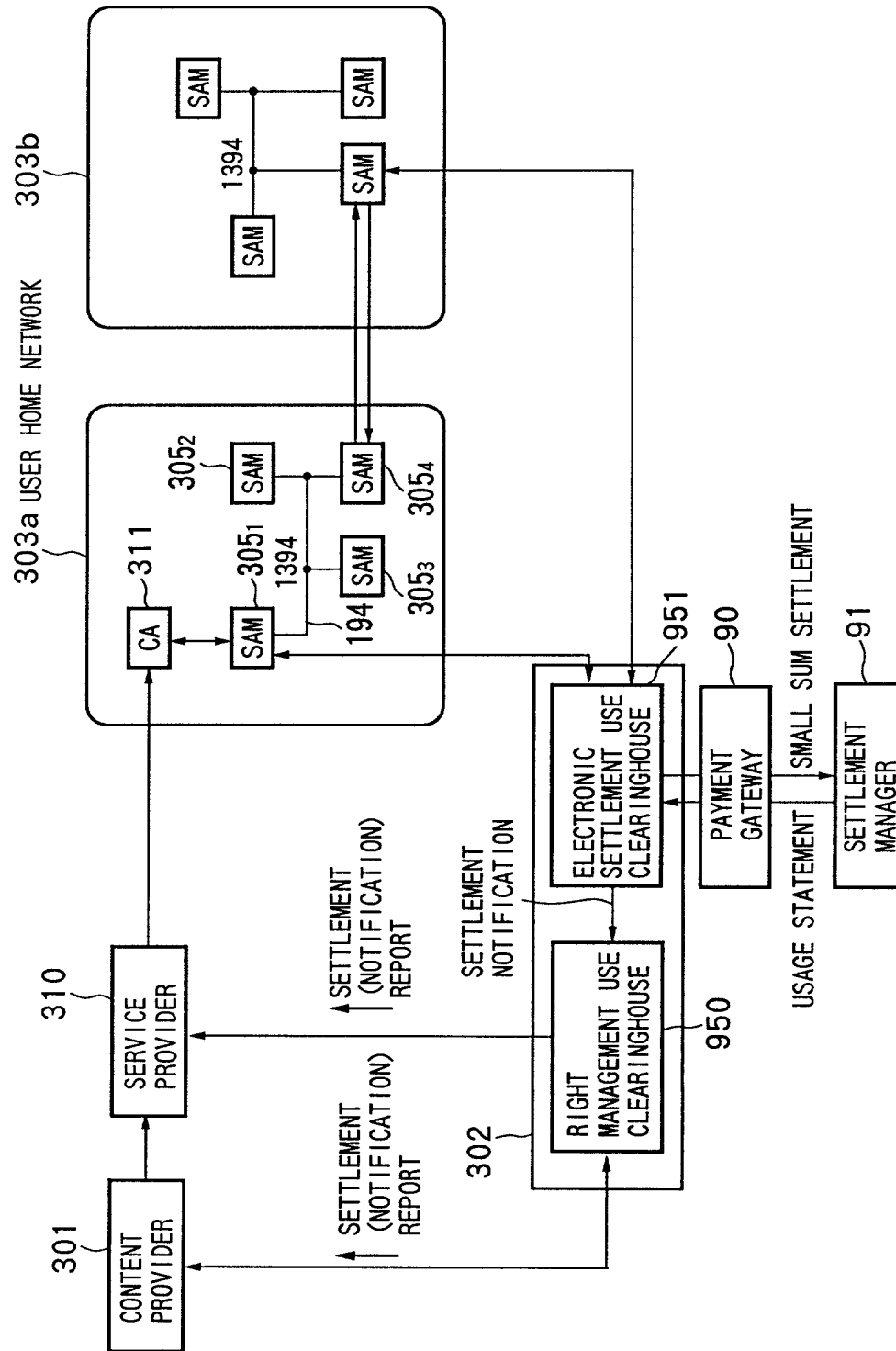


FIG.108

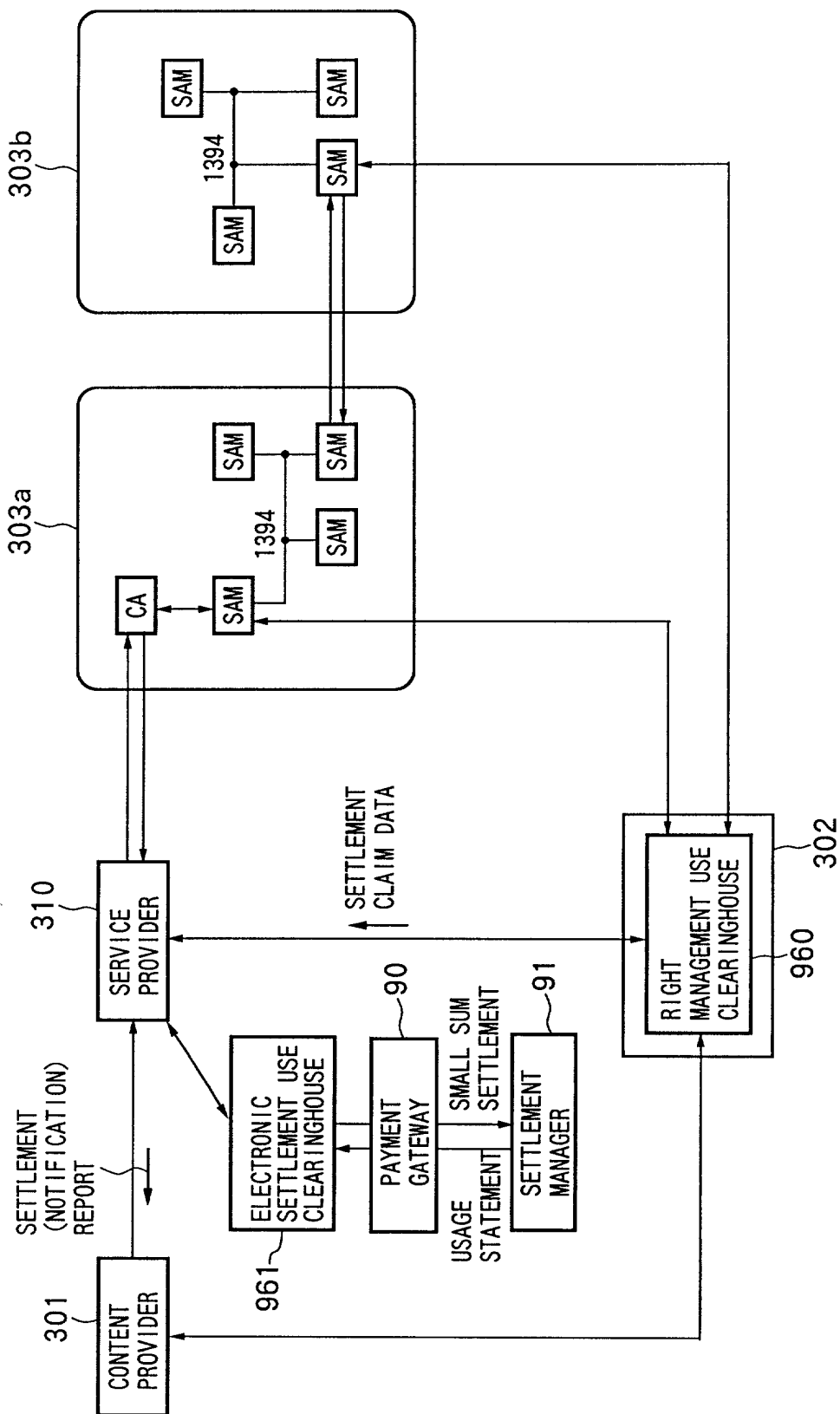




FIG. 109

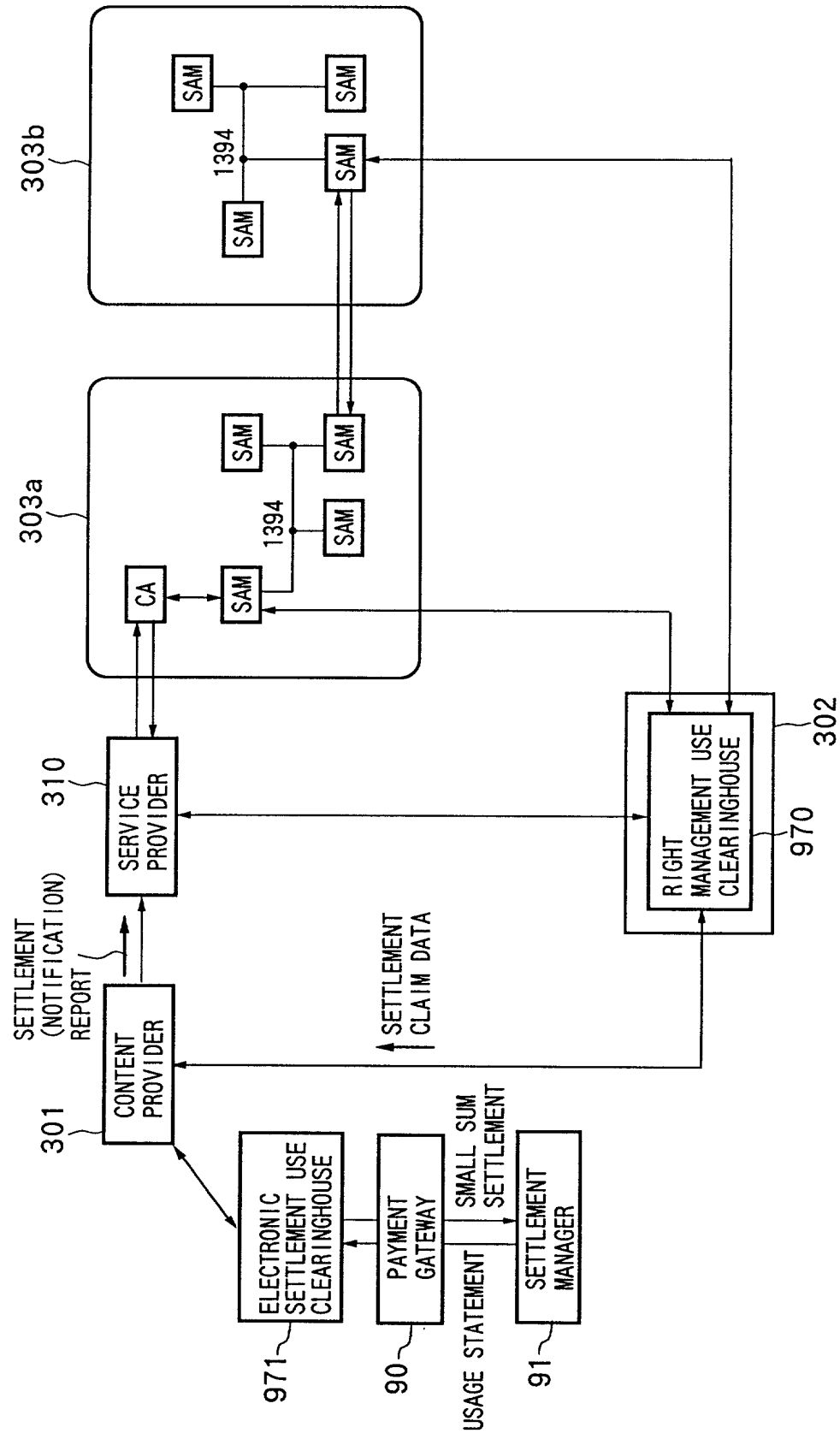
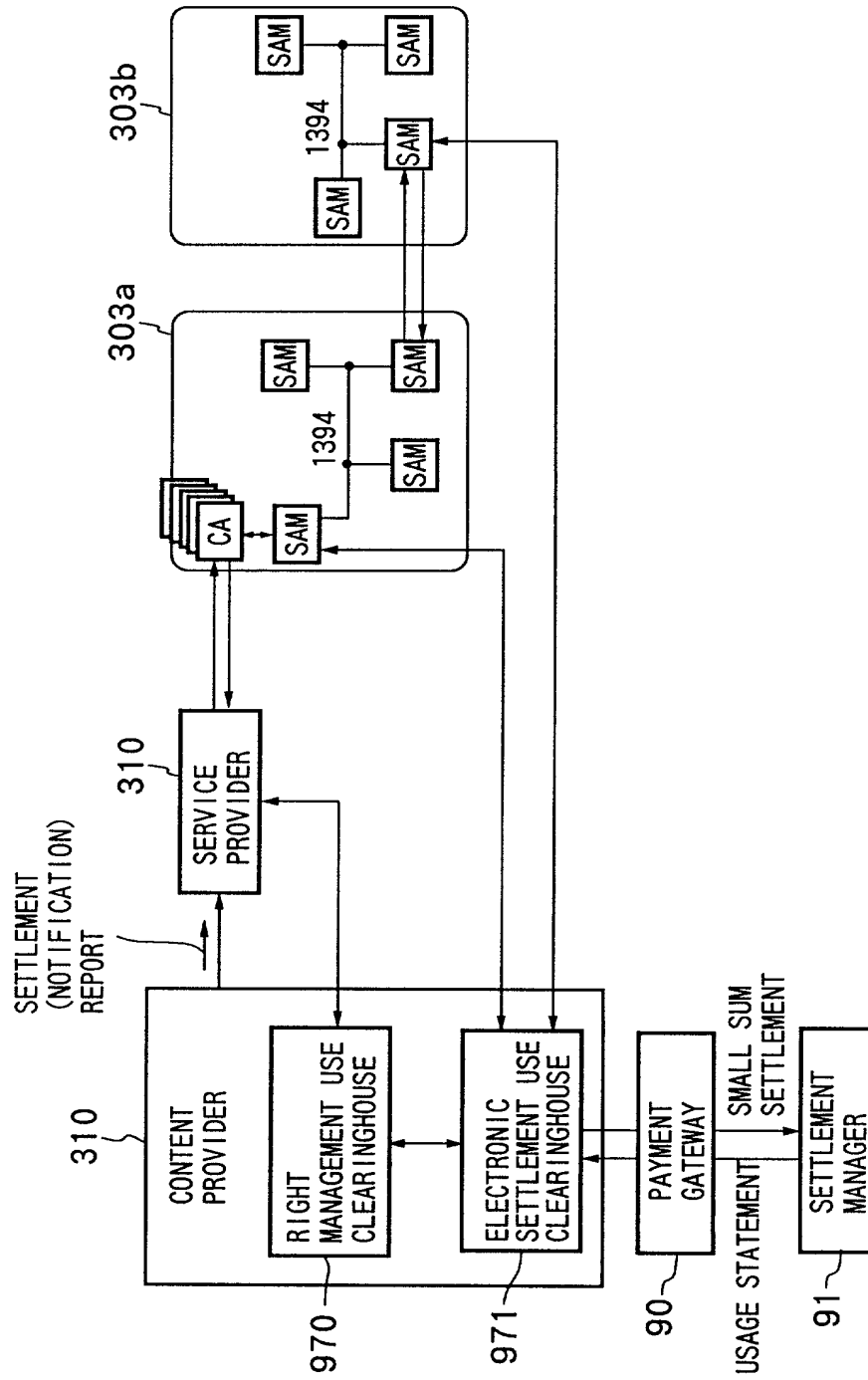


FIG.110



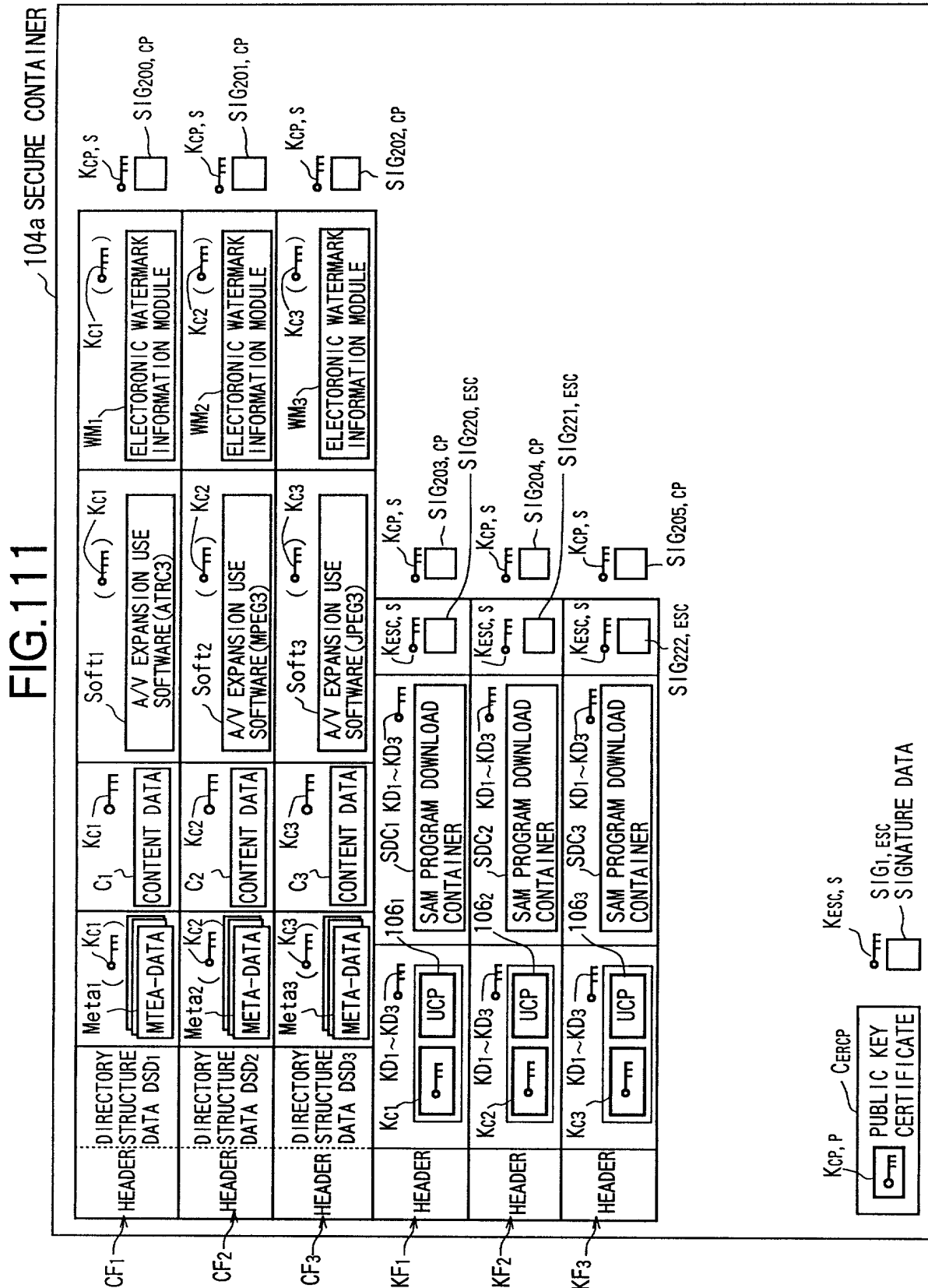


FIG.112

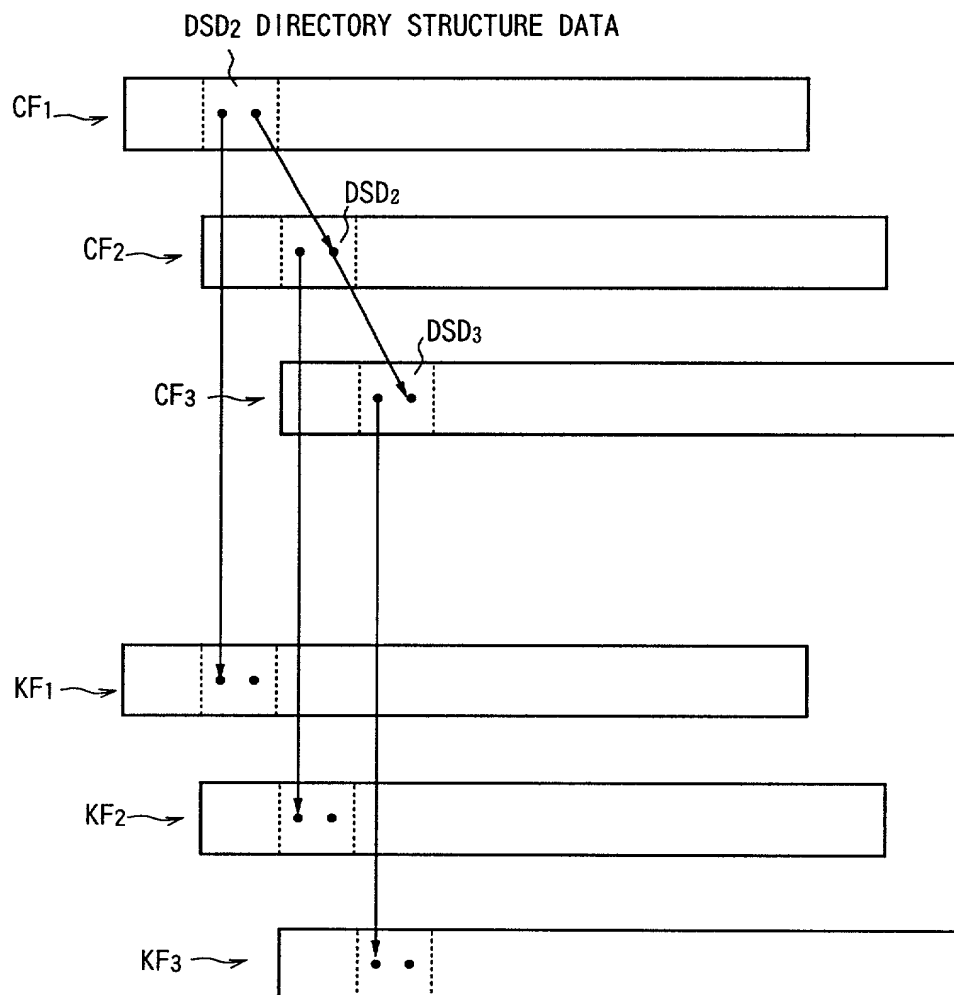
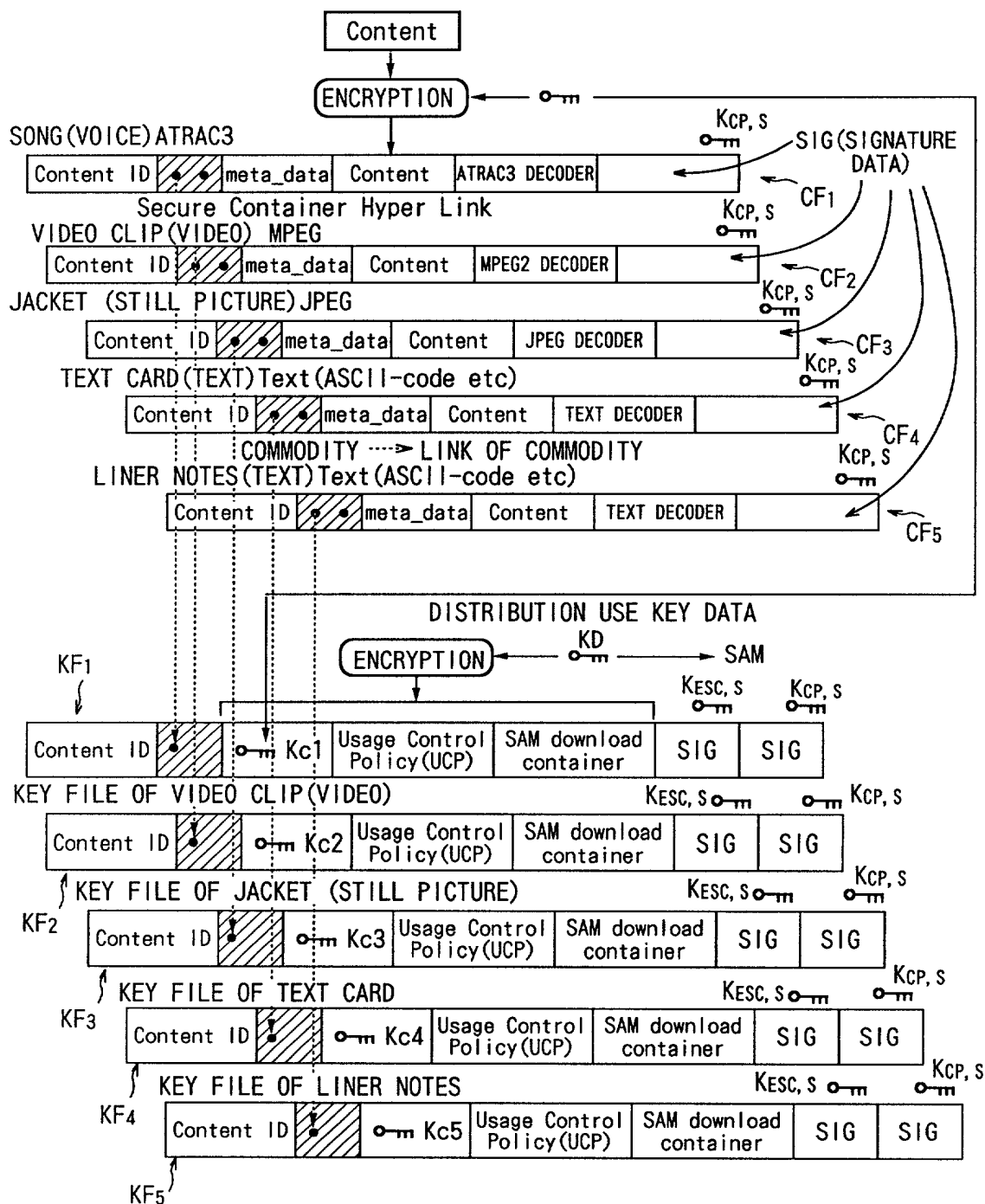


FIG.113



304a SECURE CONTAINER

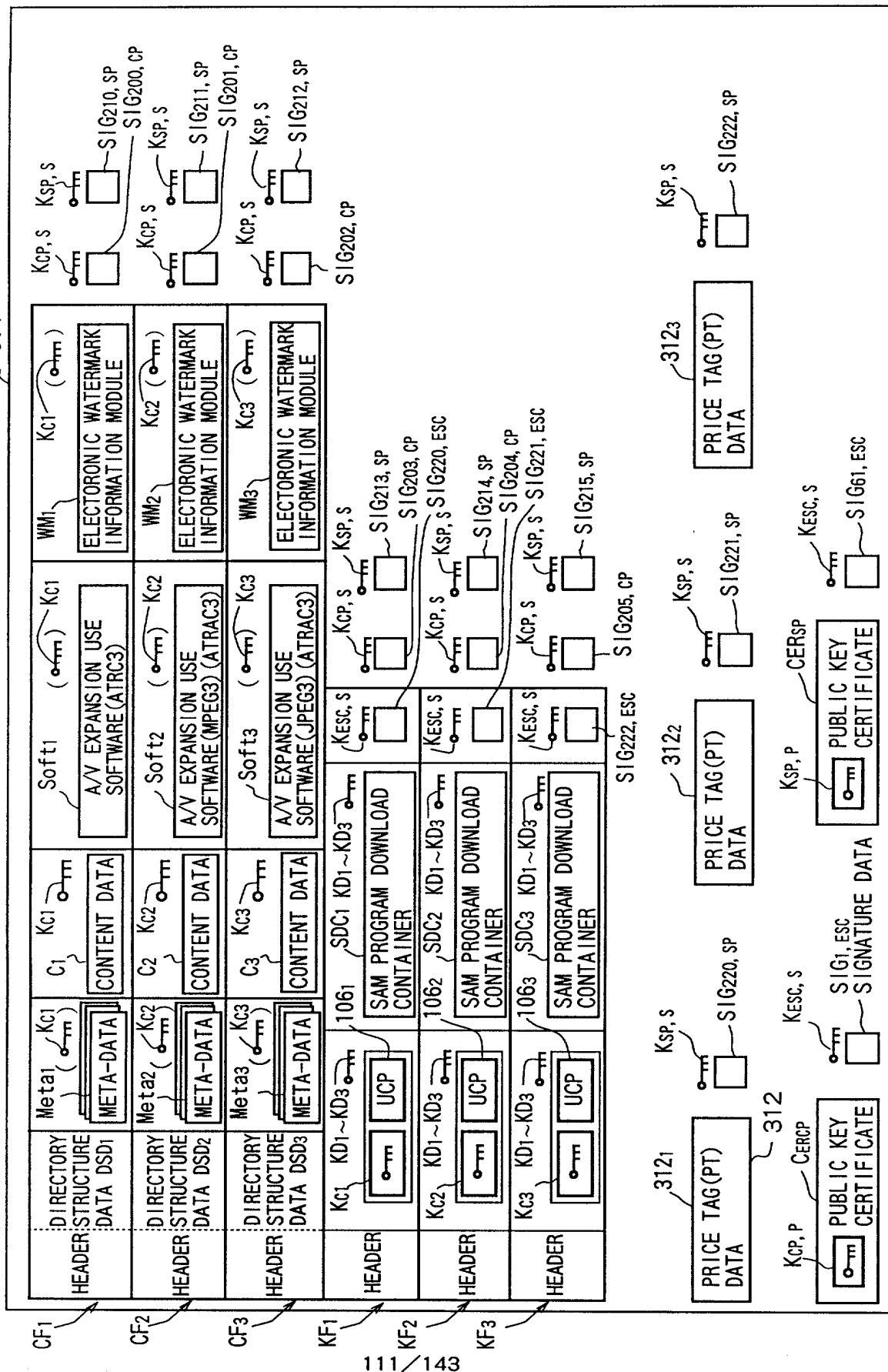


FIG.115

DATA FORMAT OF SECURE CONTAINER(COMPOSITE TYPE)-①

BASIC STRUCTURE

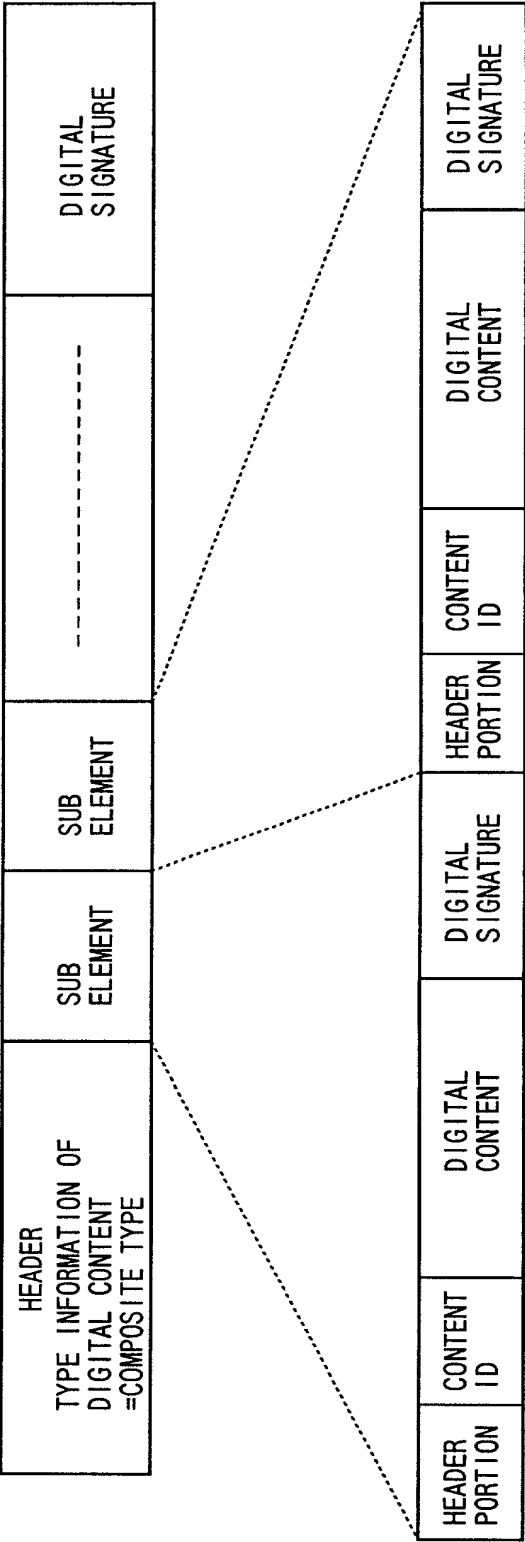


FIG.116

DATA FORMAT OF SECURE CONTAINER (COMPOSITE TYPE) - ②

HEADER PORTION	CONTENT ID	PRICE INFORMATION	SIGNATURE		
HEADER PORTION	CONTENT ID	USAGE CONTROL POLICY DATA , ETC.	HEADER PORTION	CONTENT ID	SIGNATURE
HEADER PORTION	CONTENT ID	VOICE DATA (TUNE)	HEADER PORTION	CONTENT ID	SIGNATURE
HEADER PORTION	CONTENT ID	STILL PICTURE DATA (JACKET)	HEADER PORTION	CONTENT ID	SIGNATURE
SIGNATURE					



FIG. 117

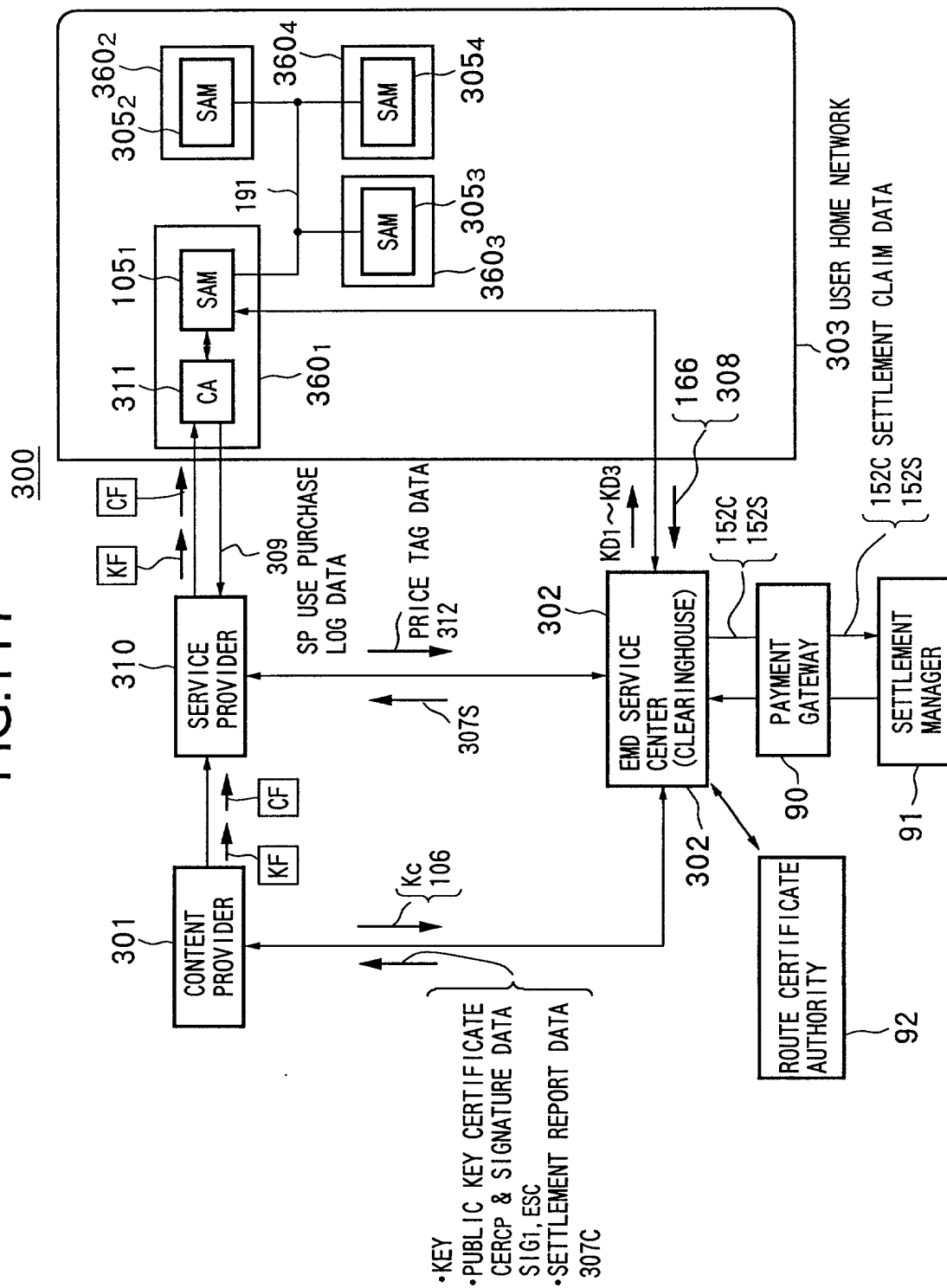


FIG.118

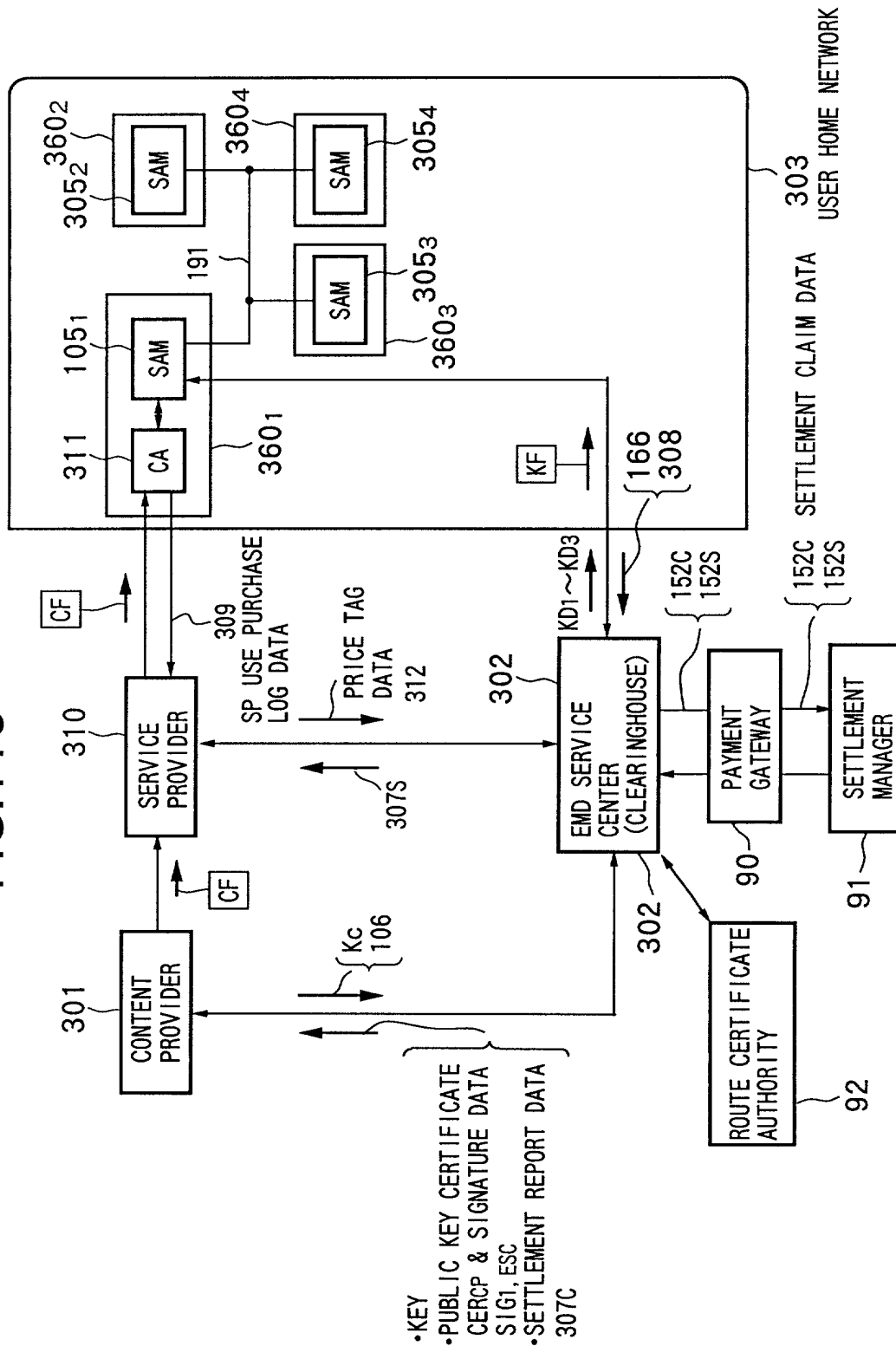


FIG.119

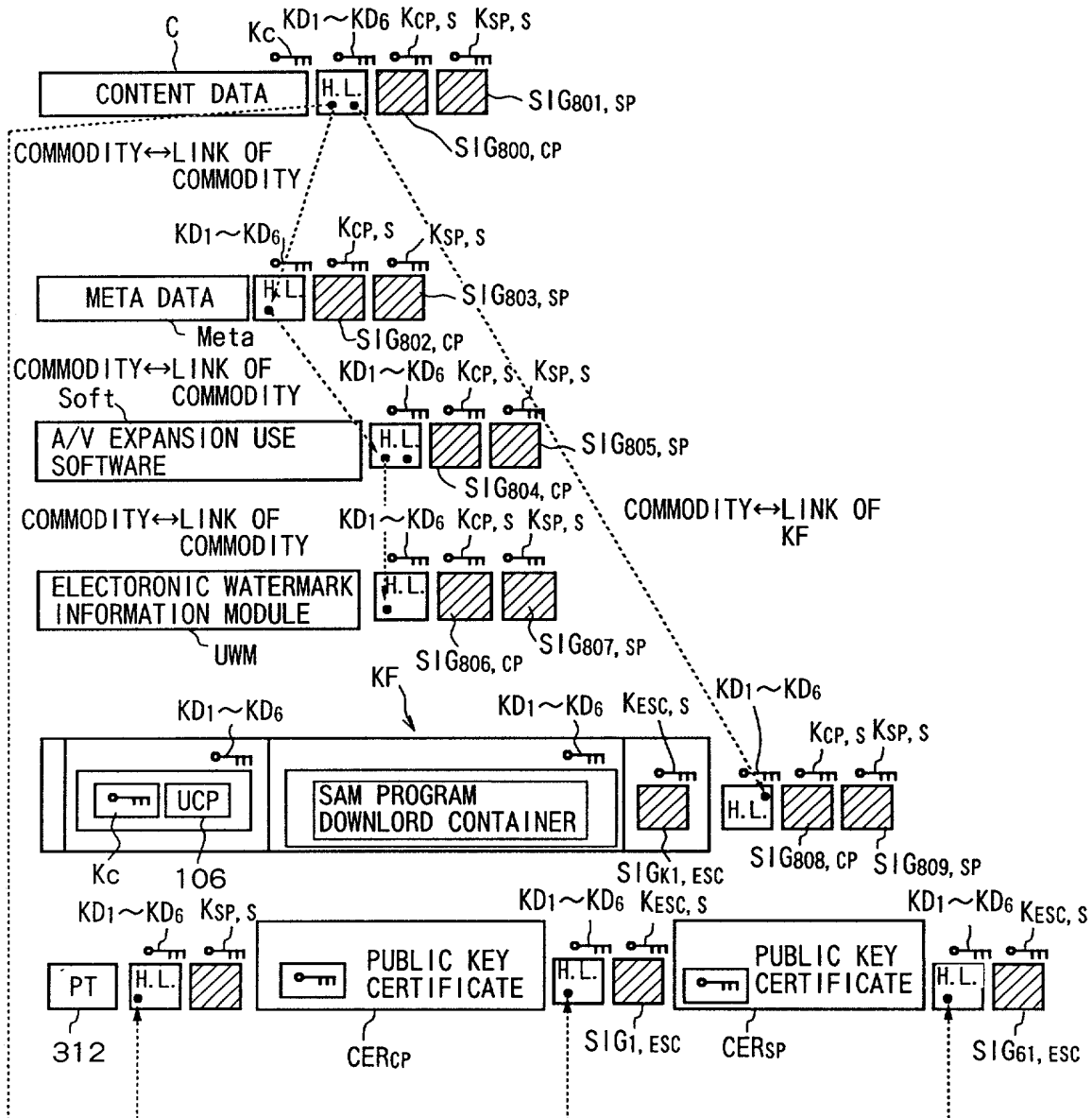


FIG.120

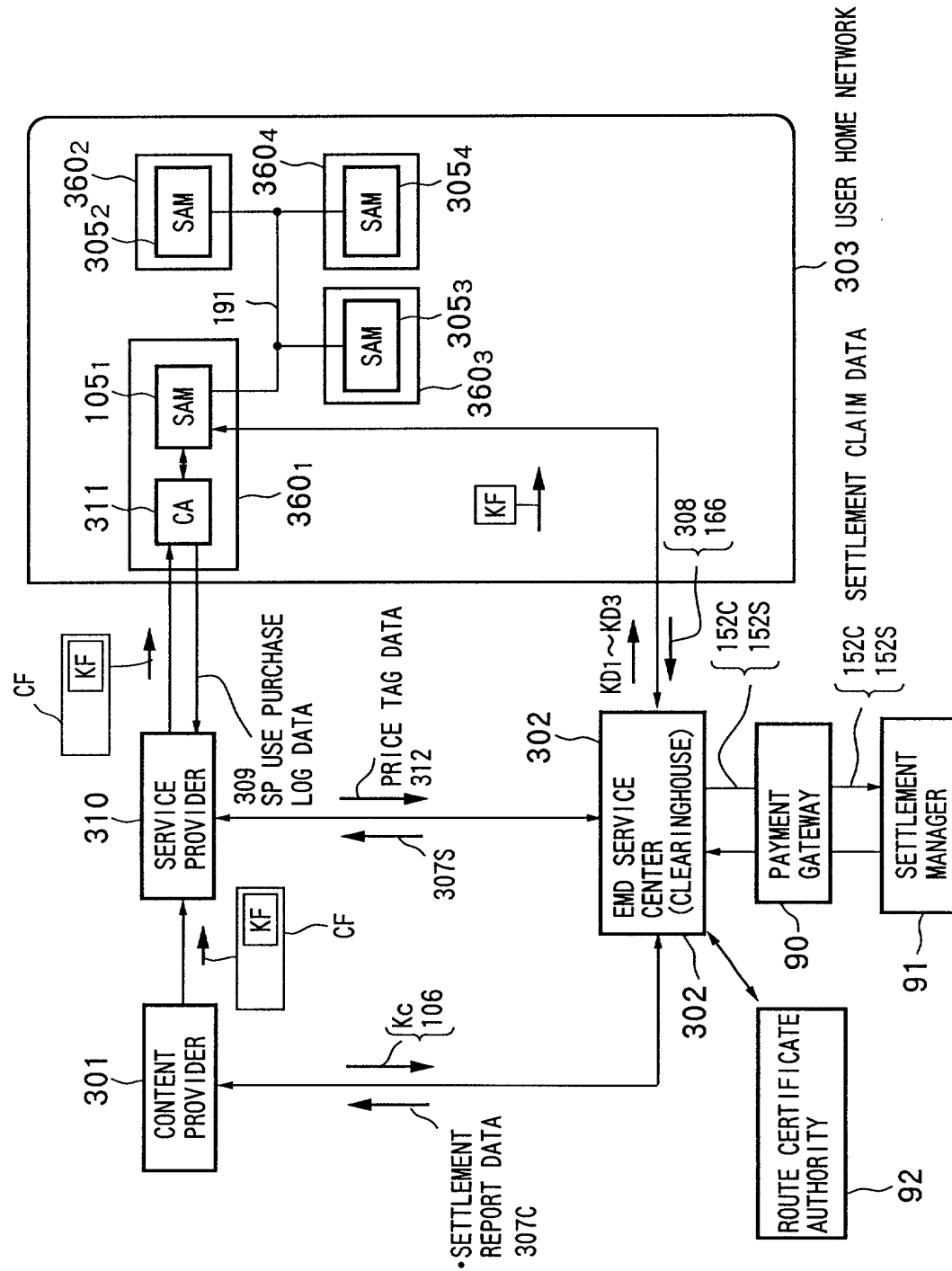


FIG.121

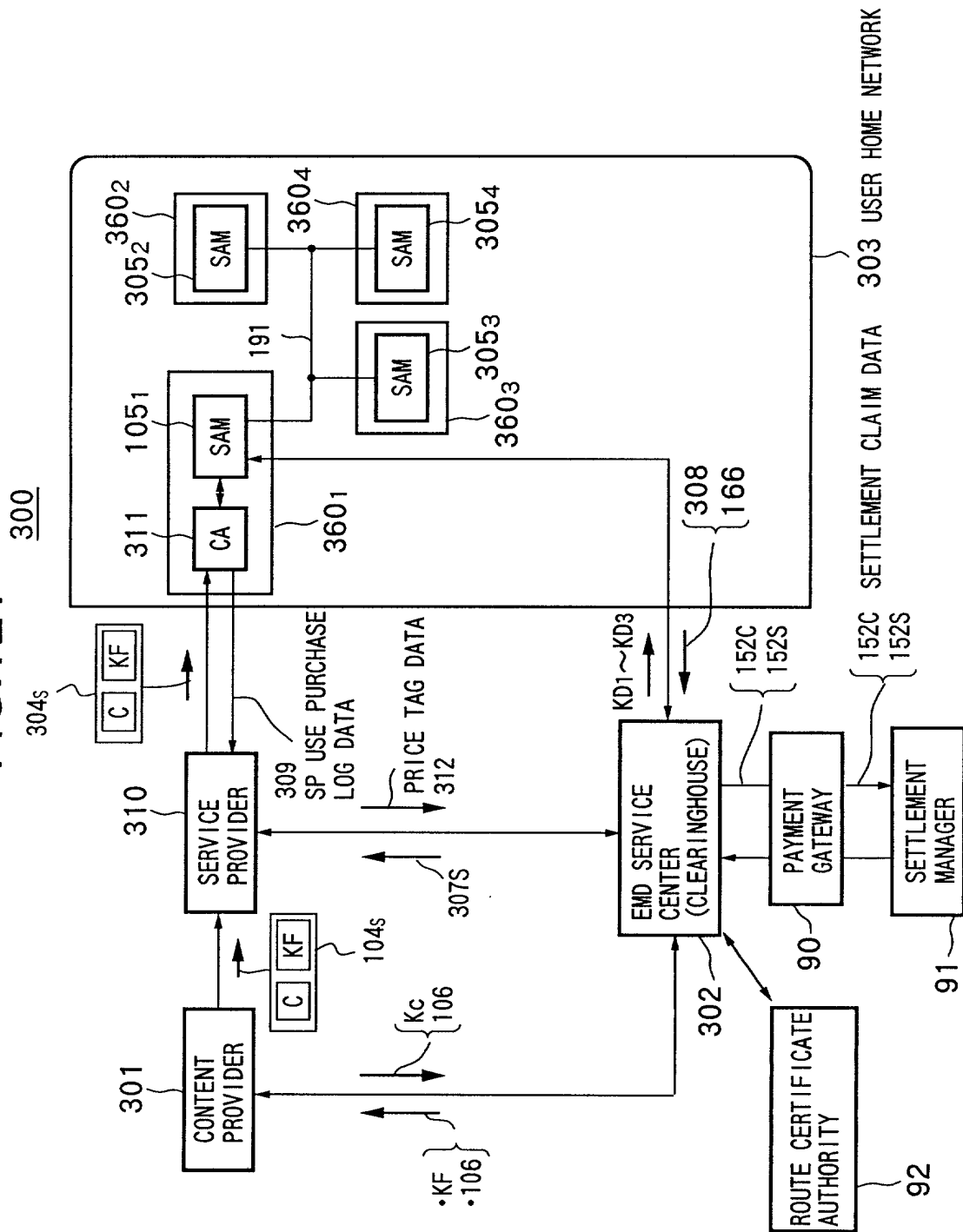


FIG.122

300

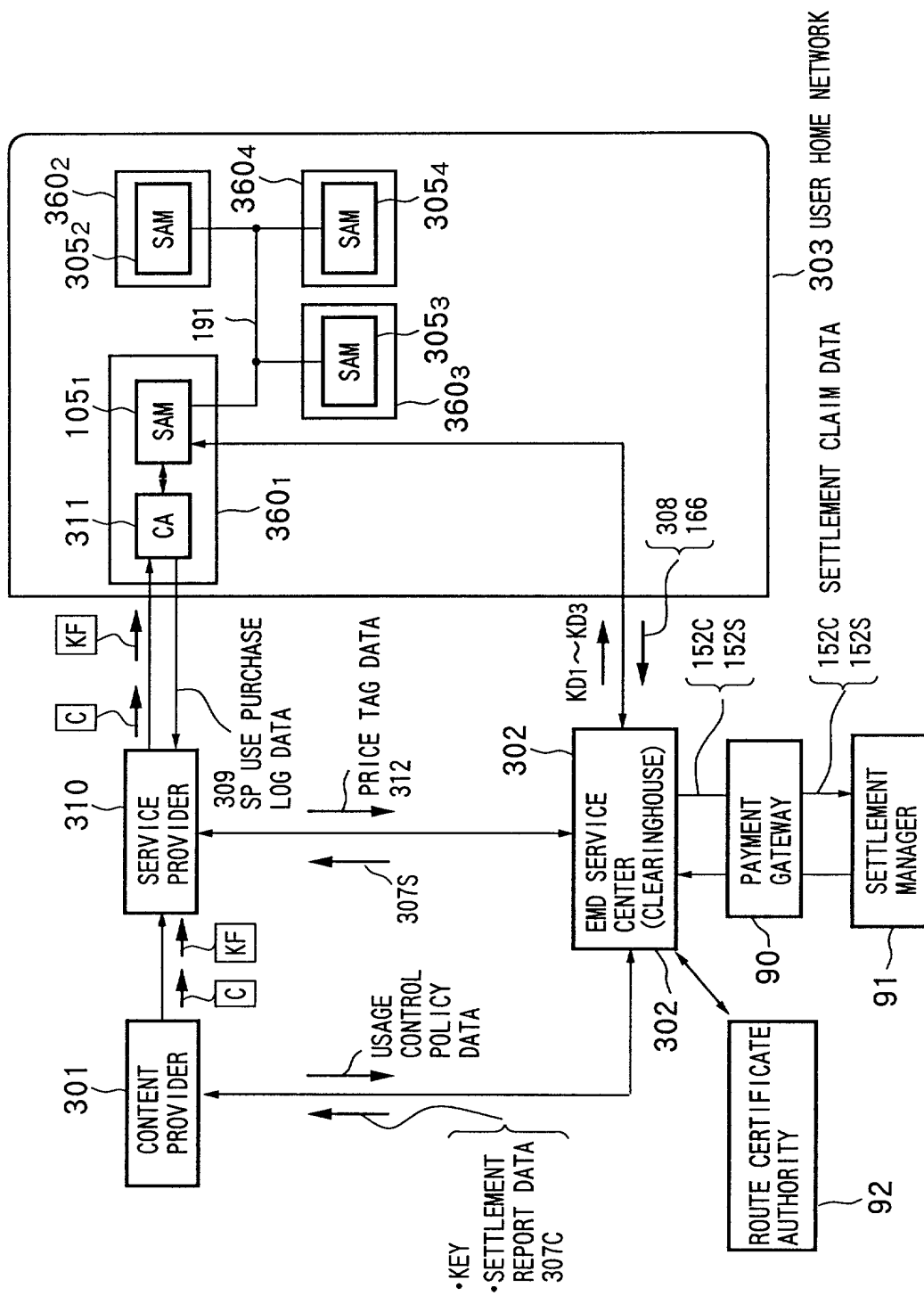


FIG. 123

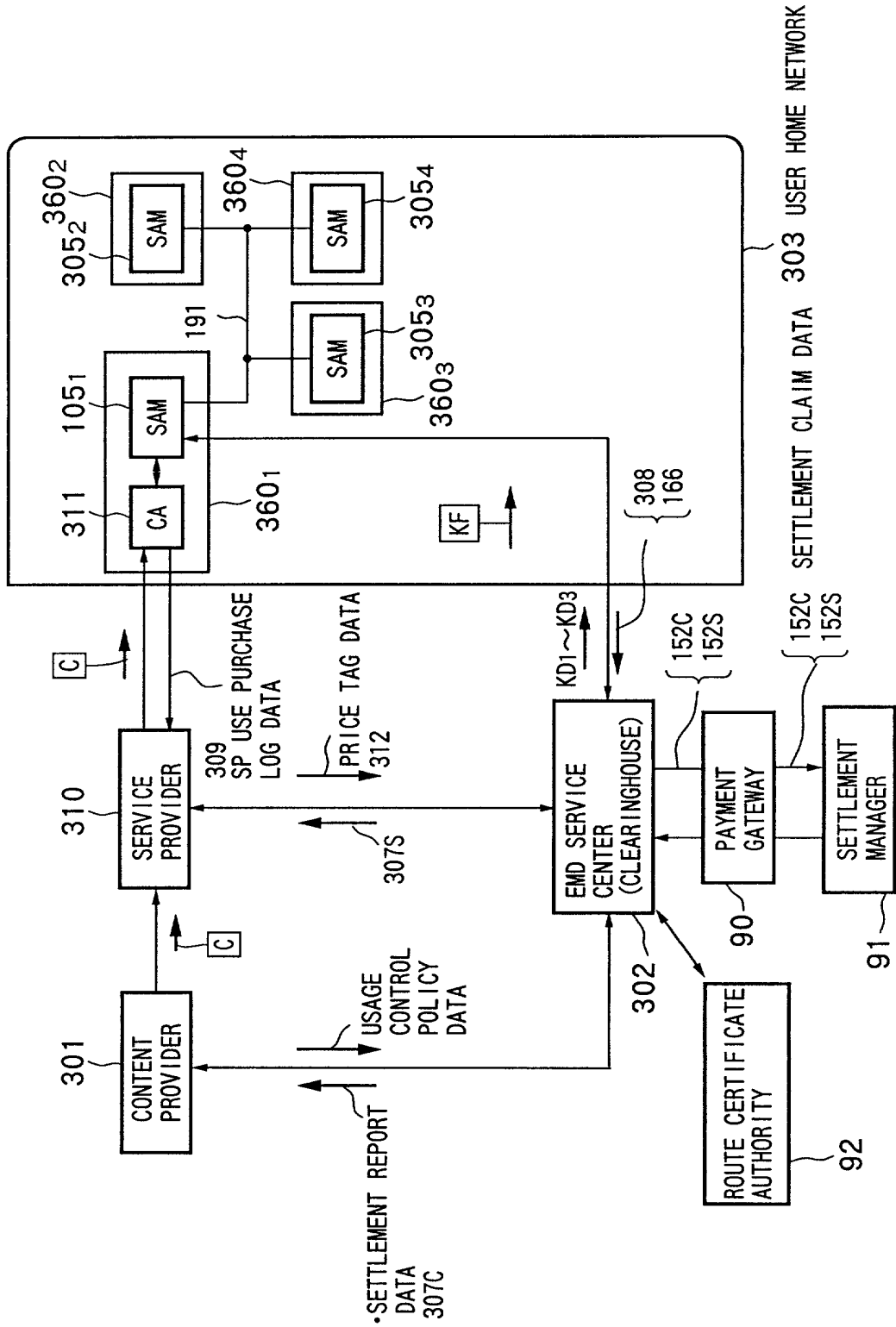


FIG.124

300

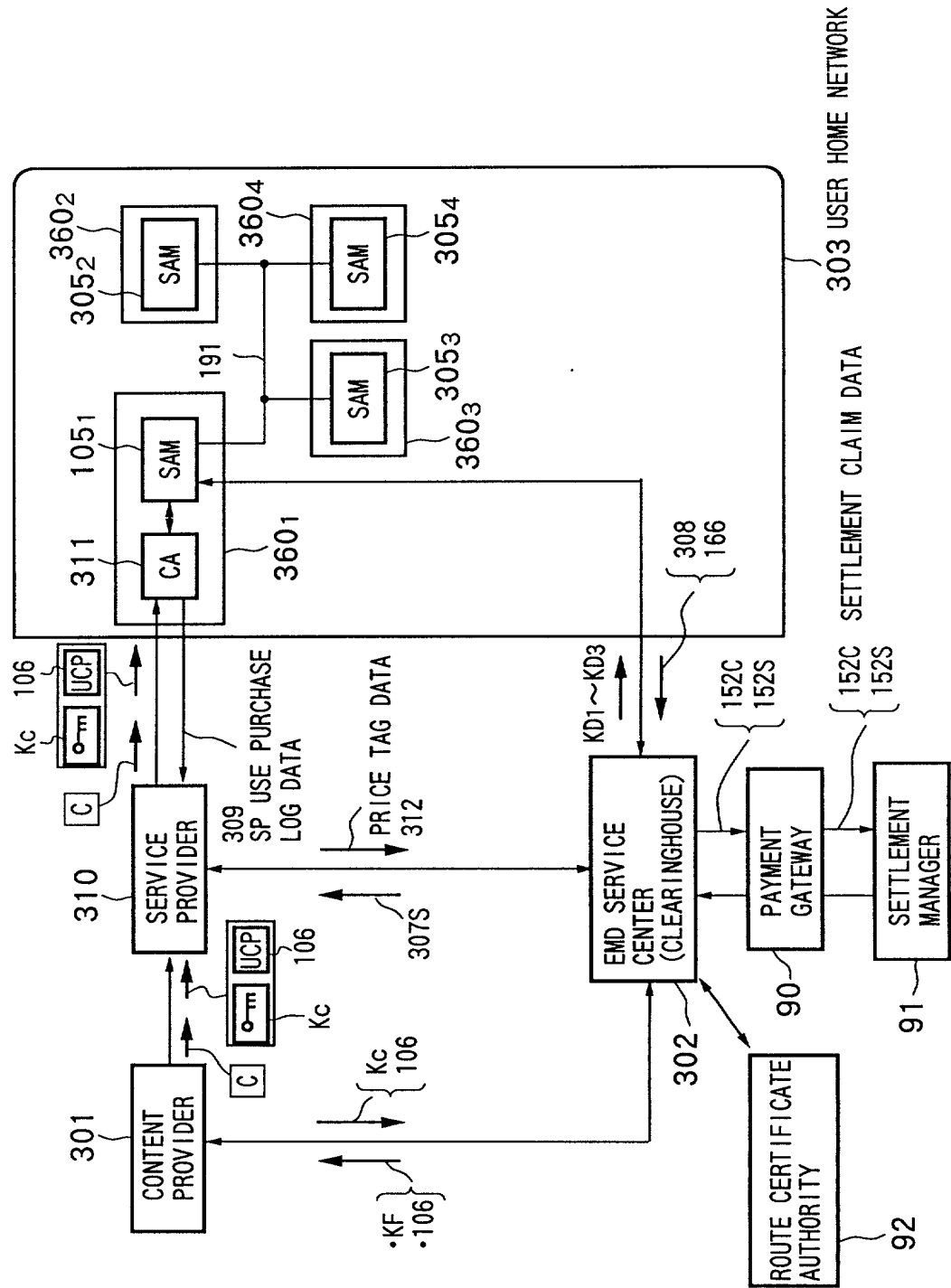
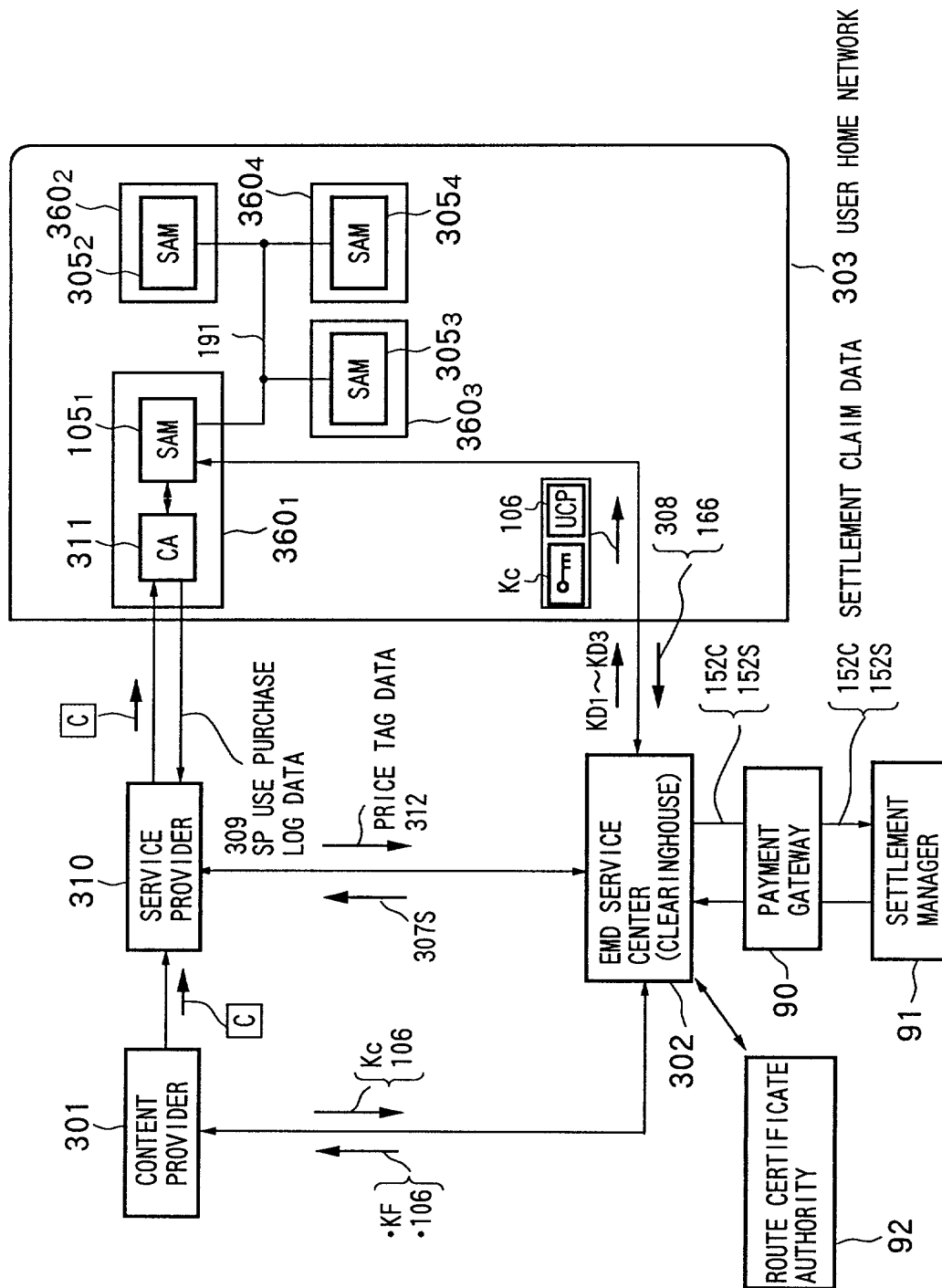




FIG.125



**FIG. 126**



FIG. 127

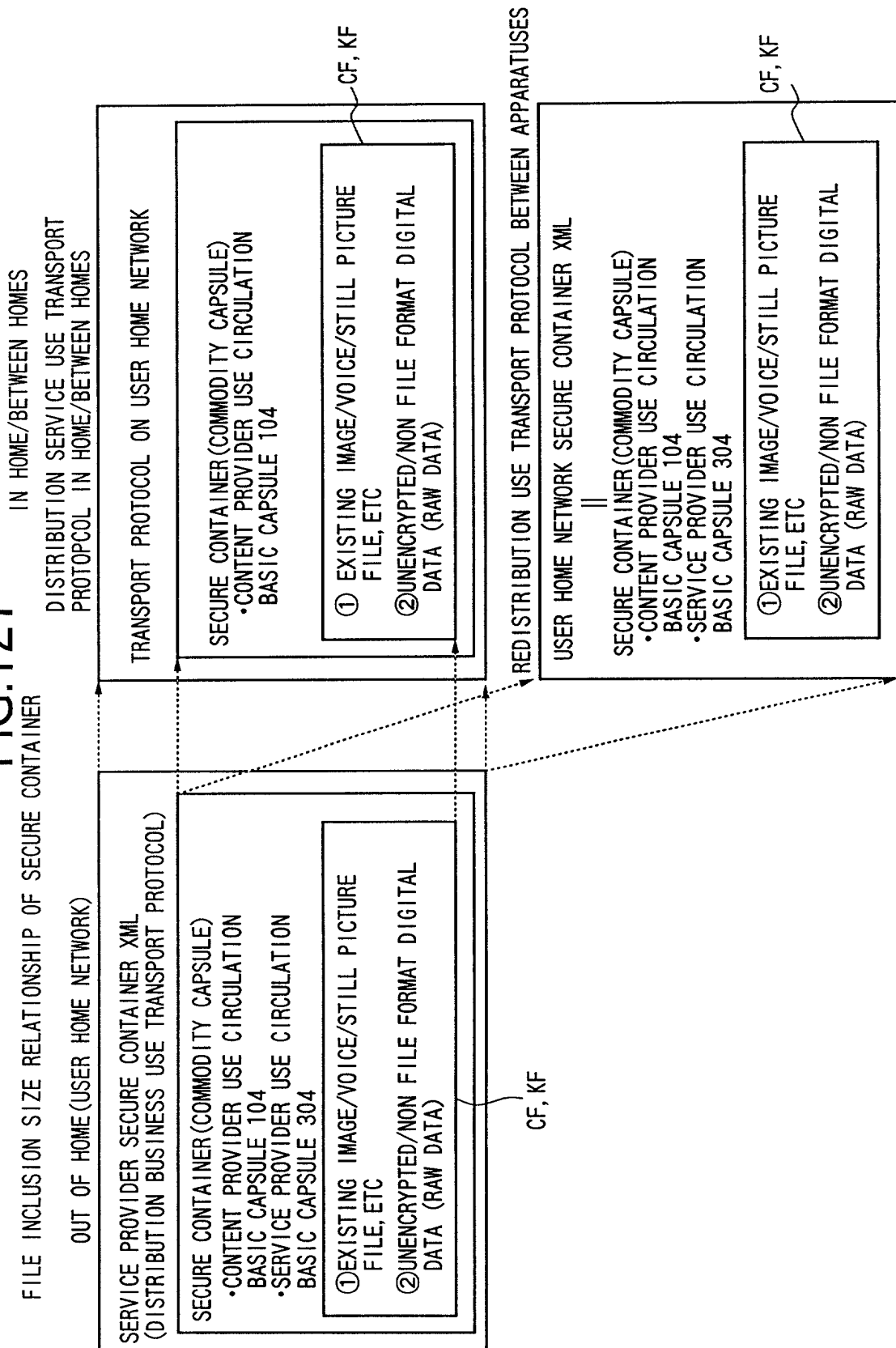
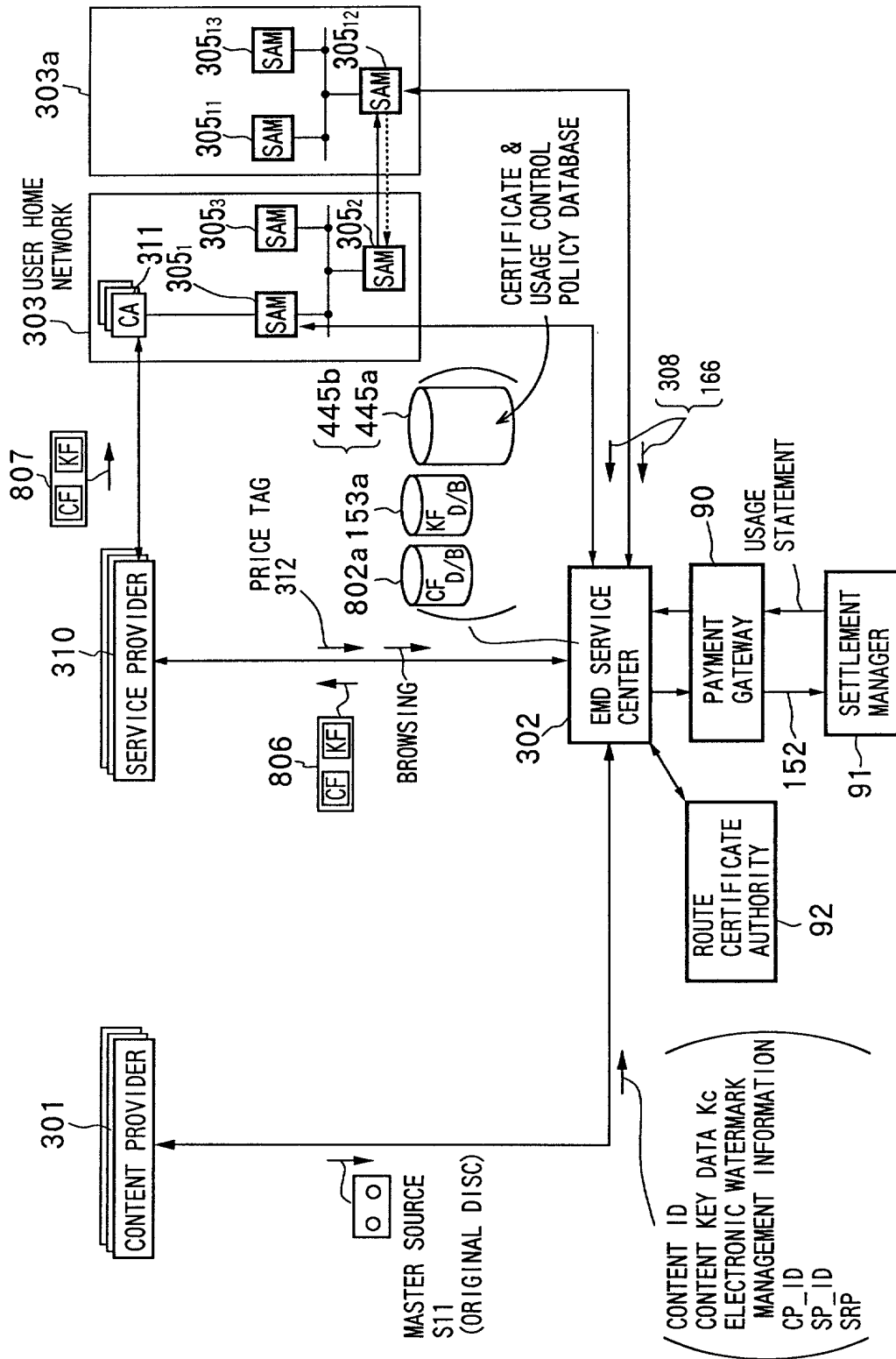


FIG. 128



**FIG. 129**

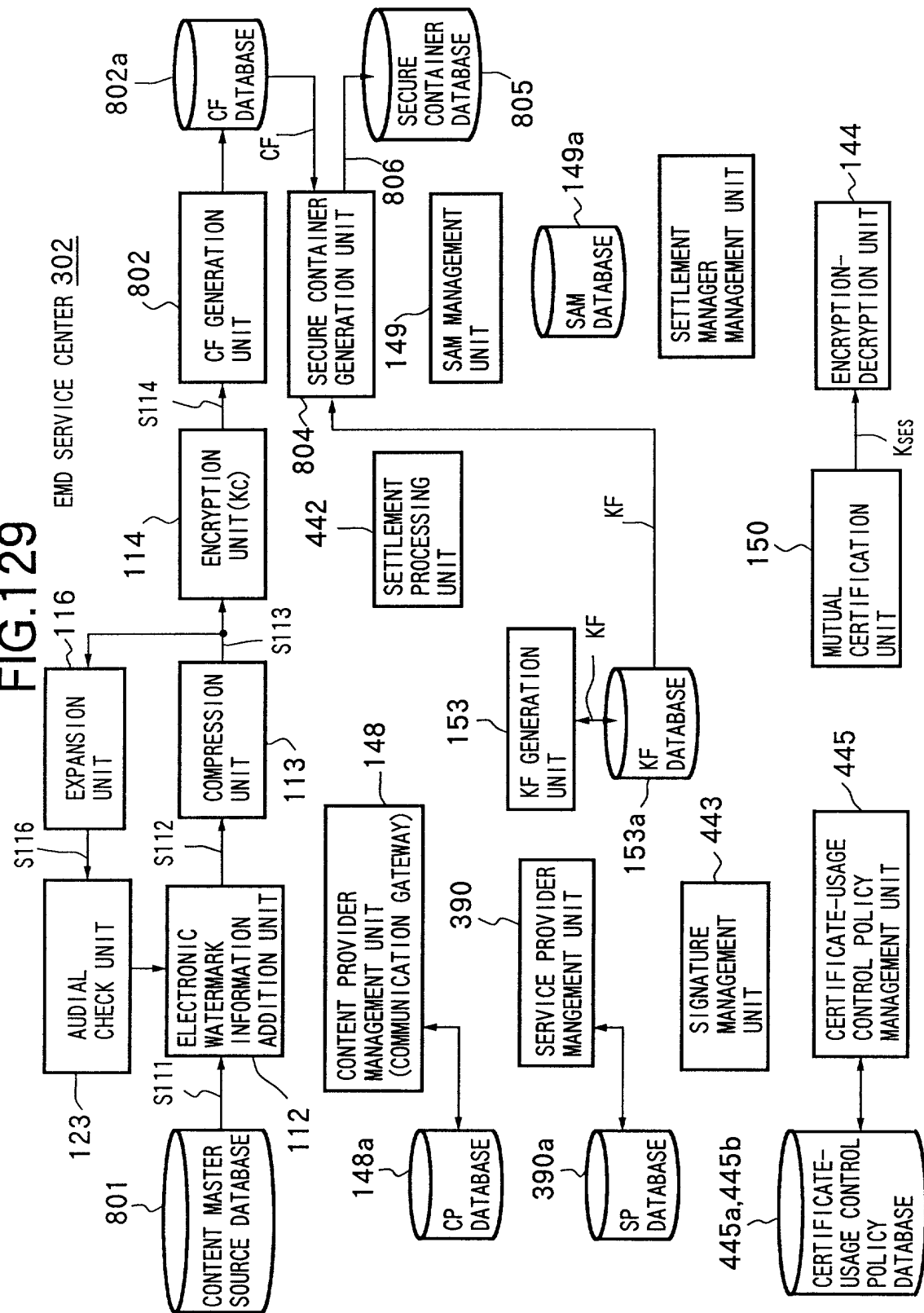
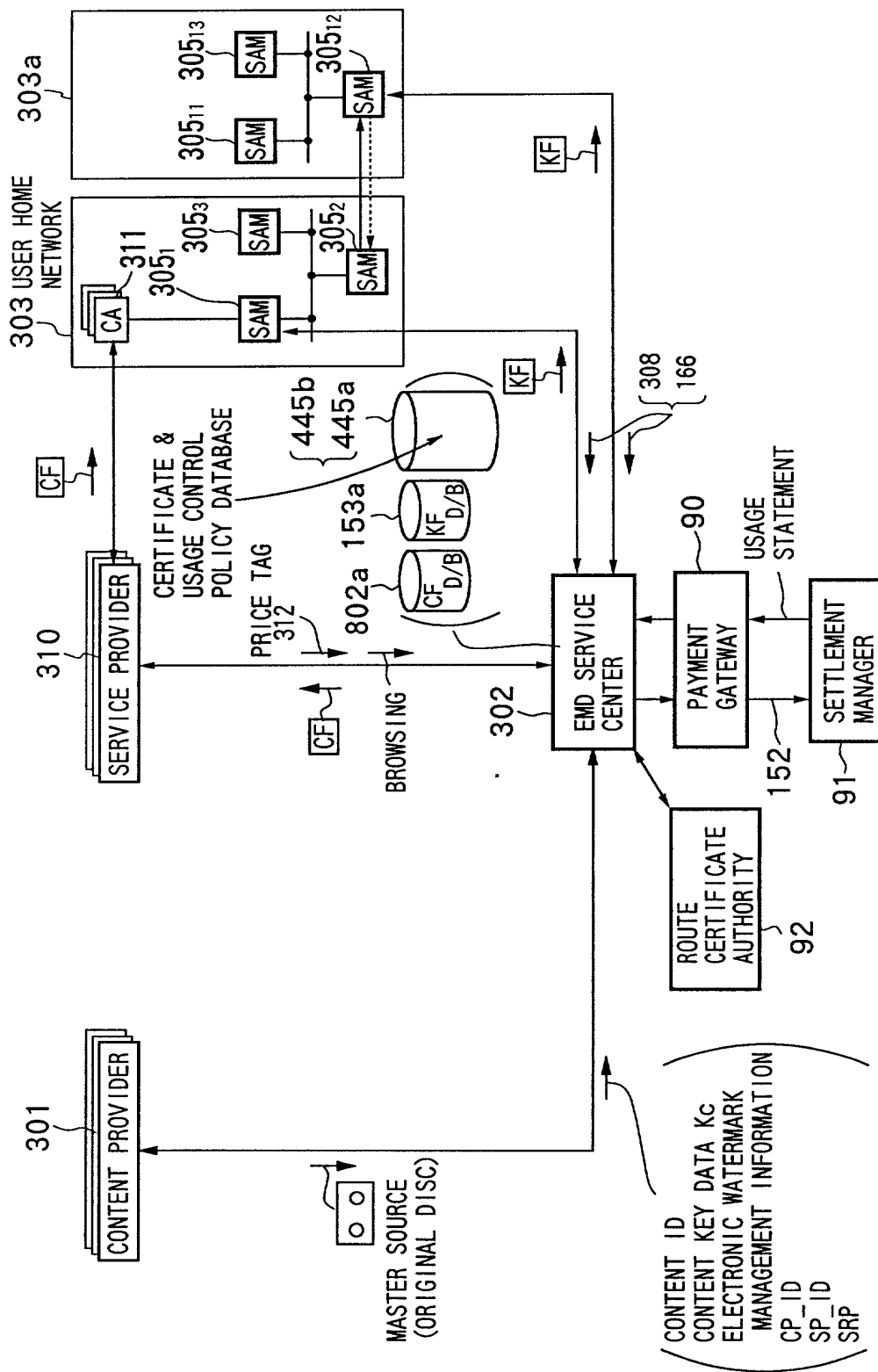


FIG. 130



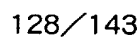
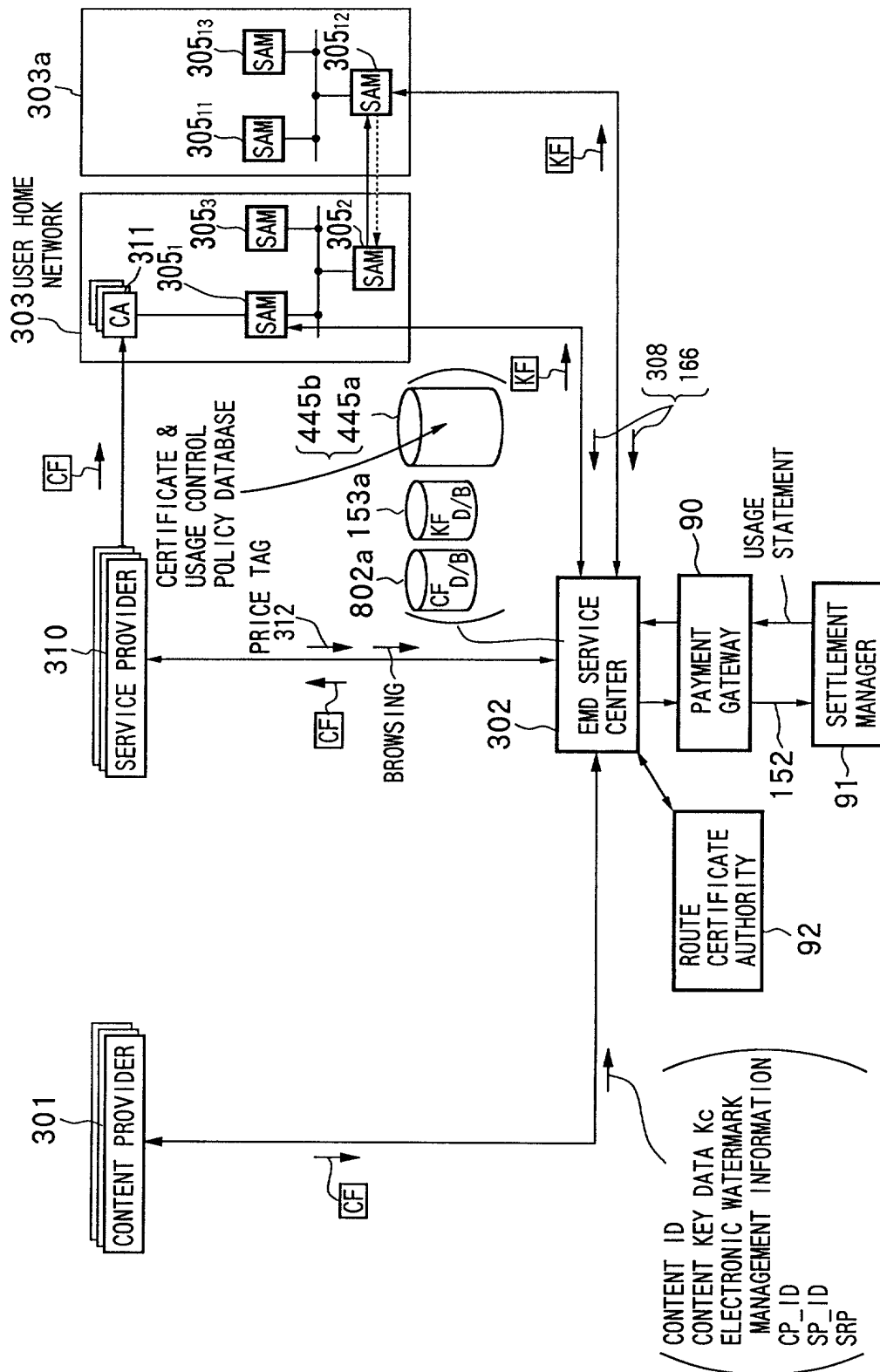


FIG. 132





**FIG. 133**

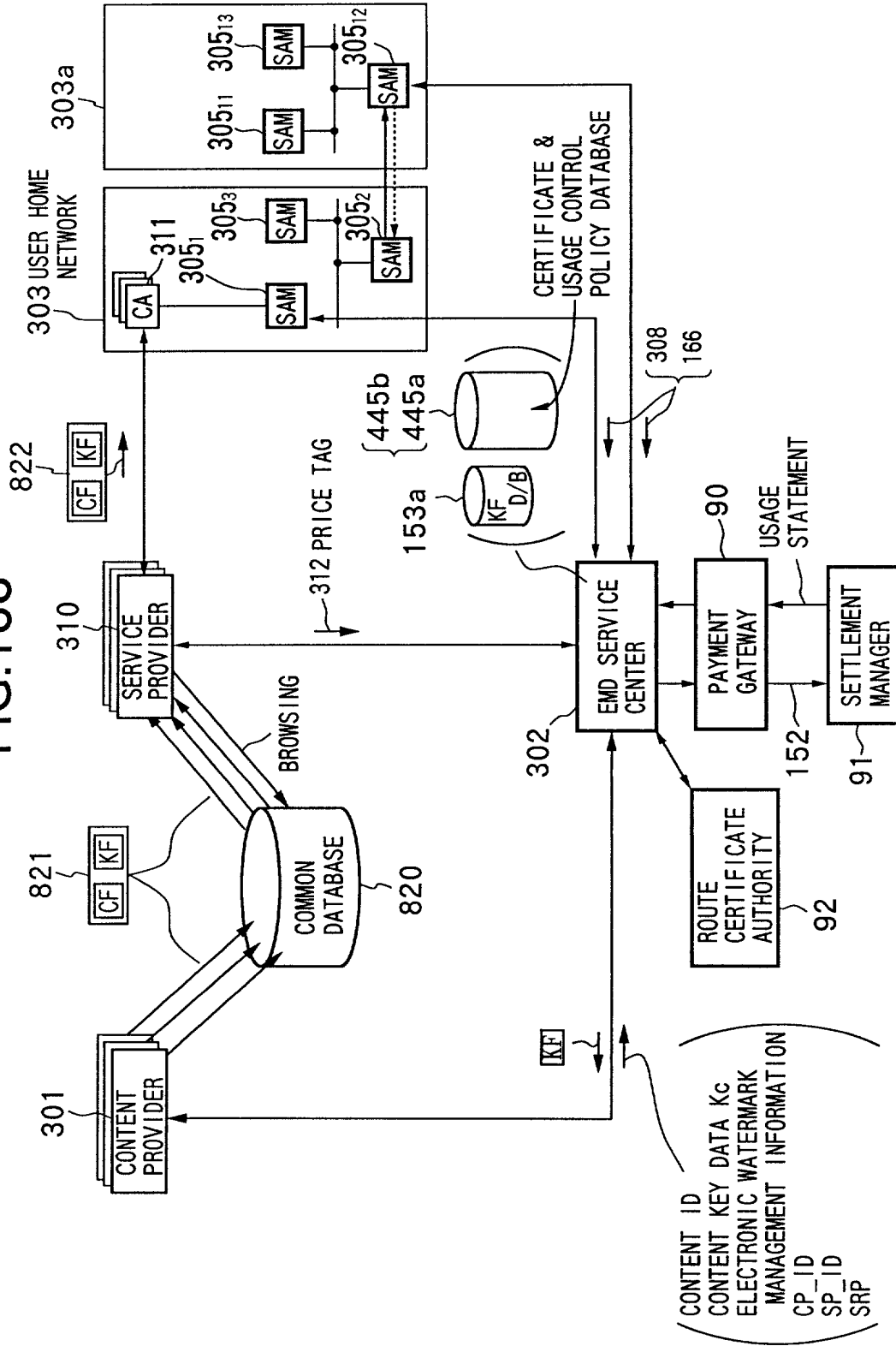
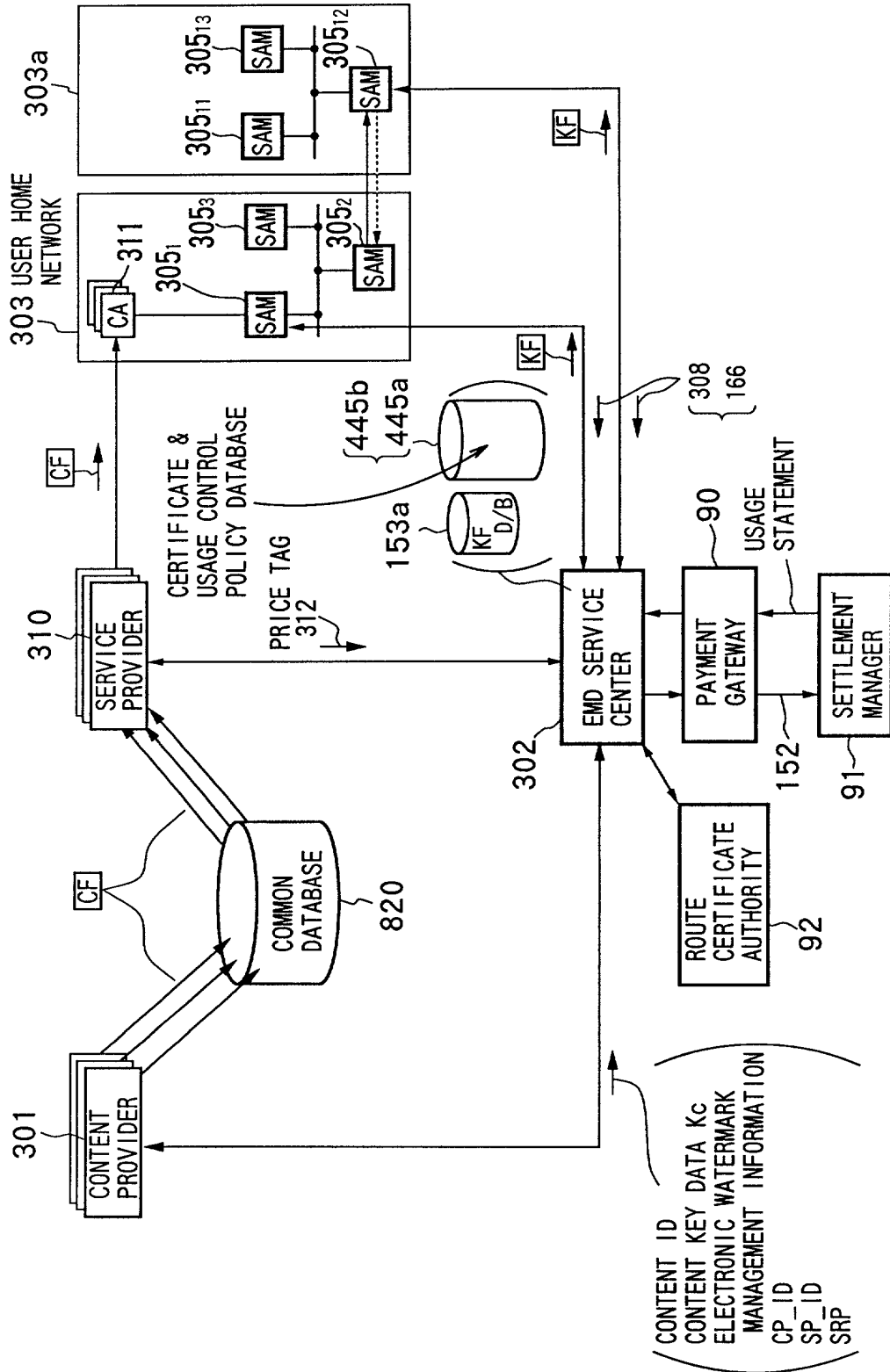




FIG. 135



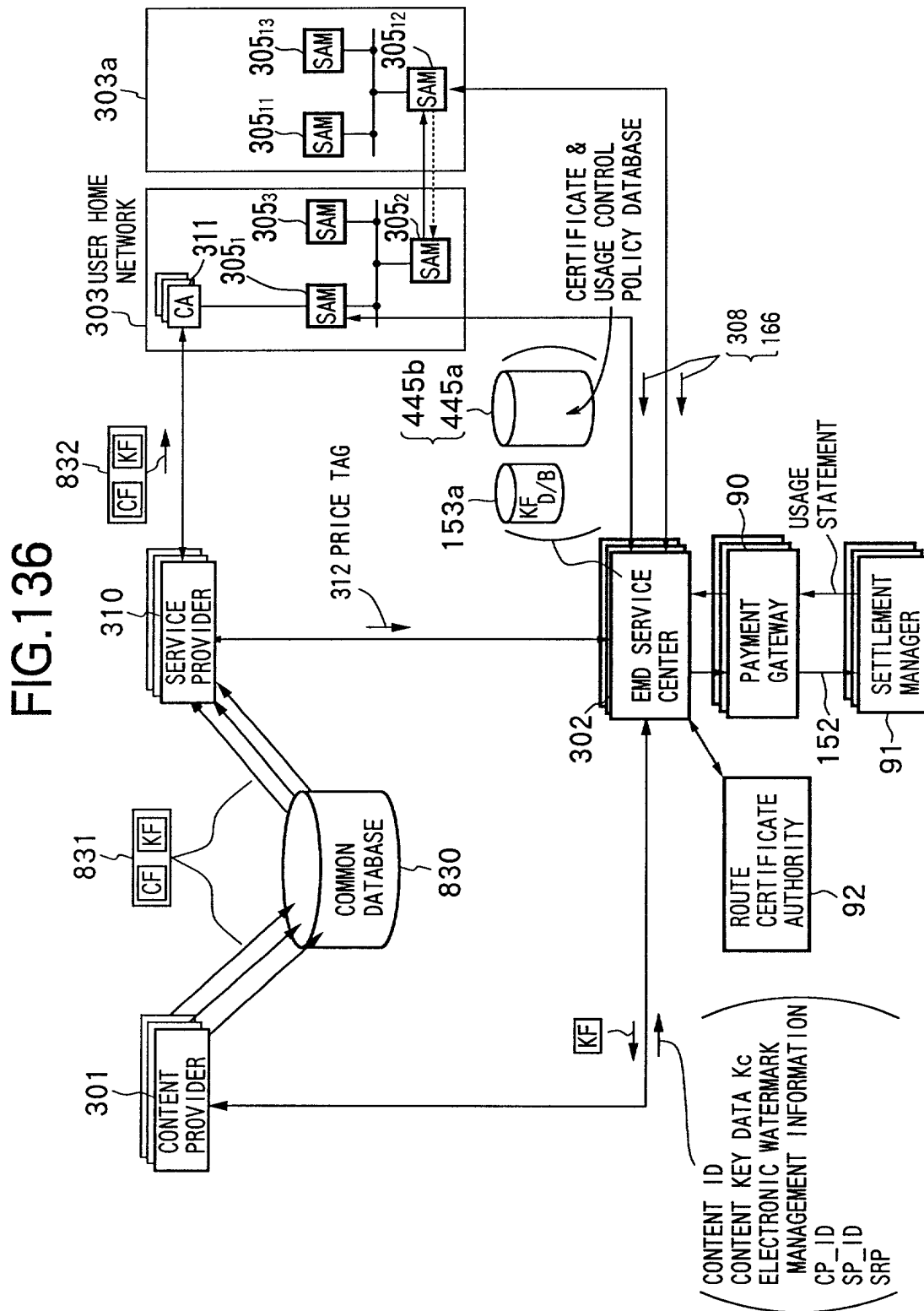
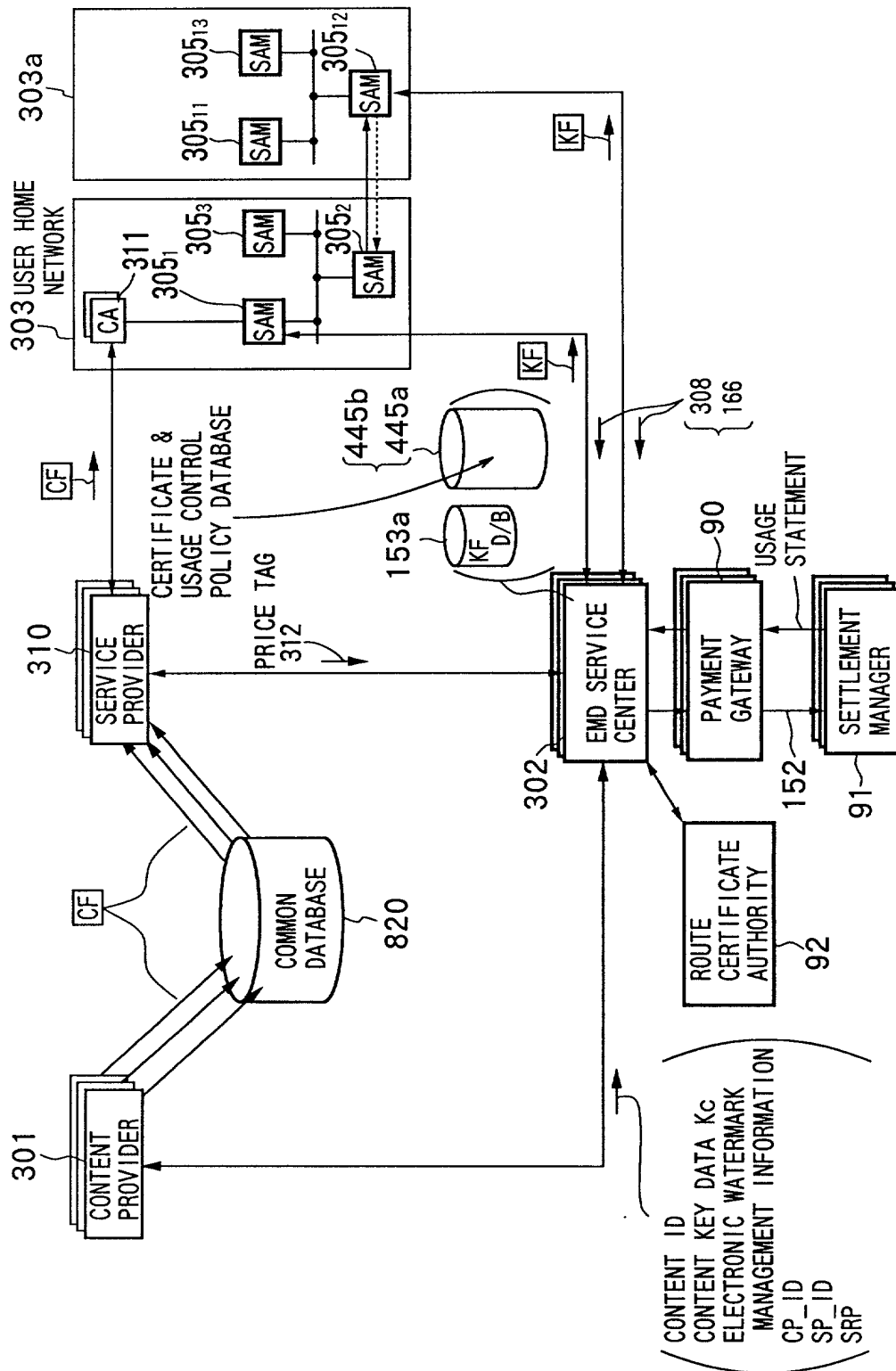




FIG. 138



**FIG. 139**

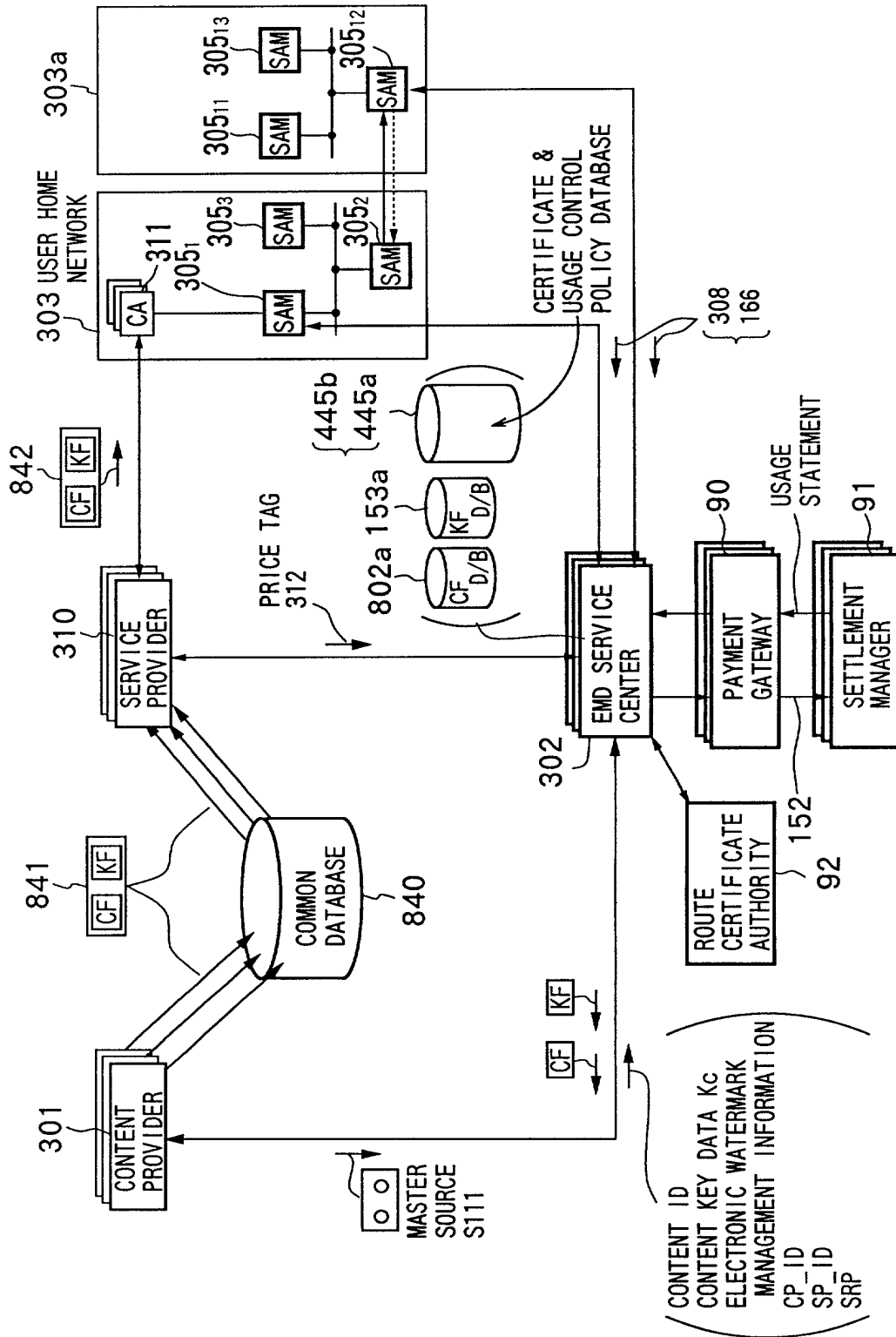


FIG.140

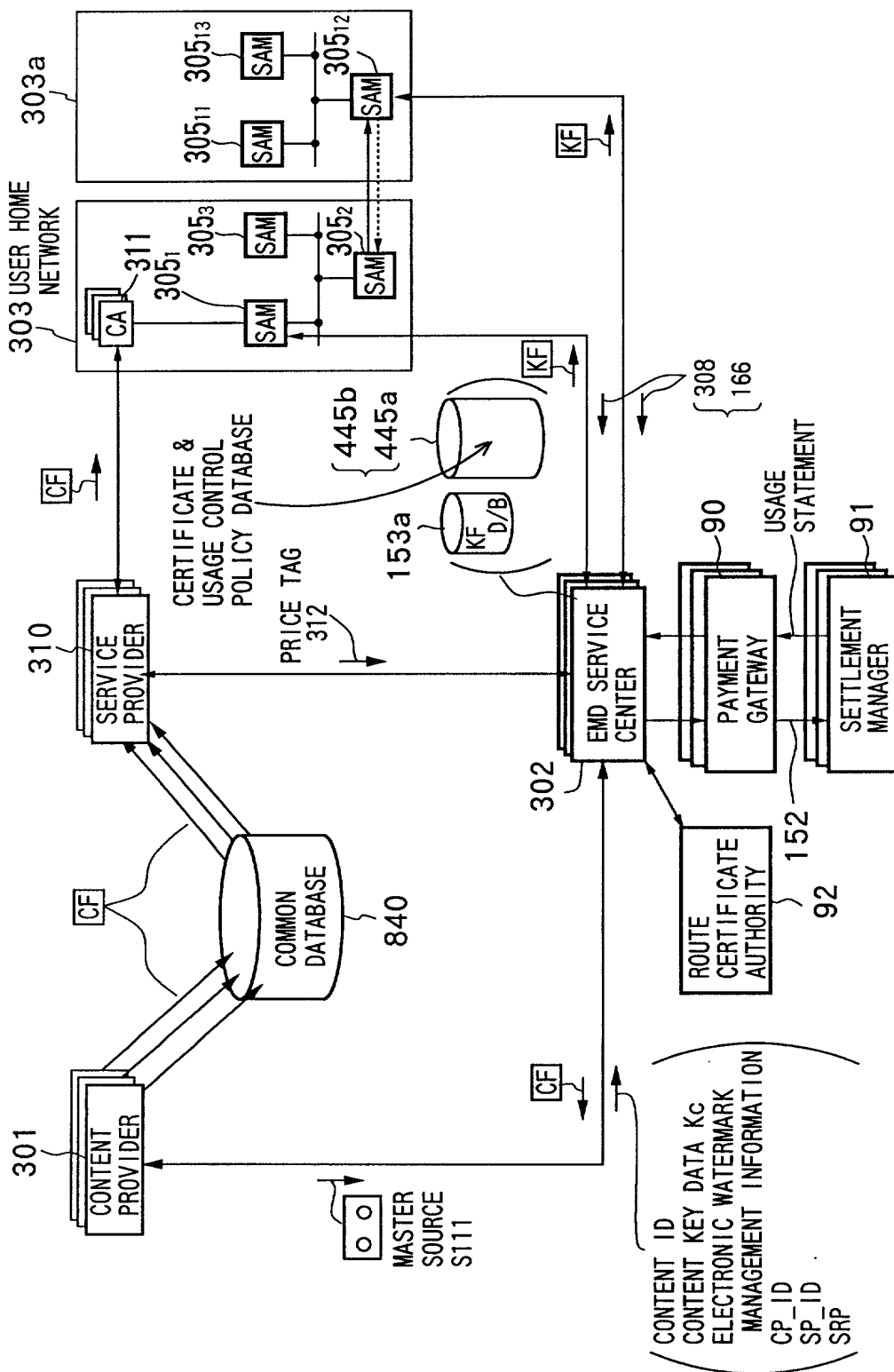








FIG. 143

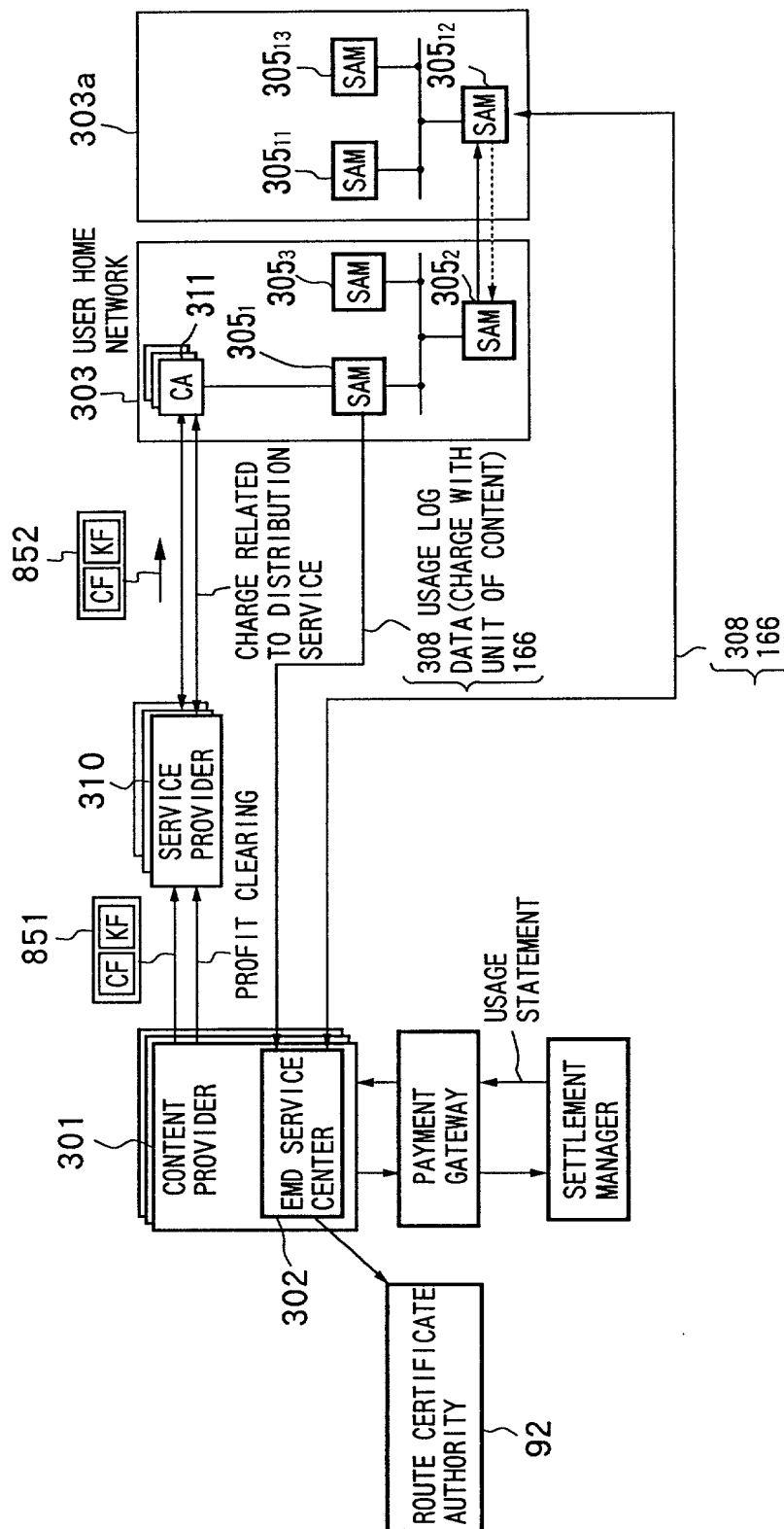


FIG.144

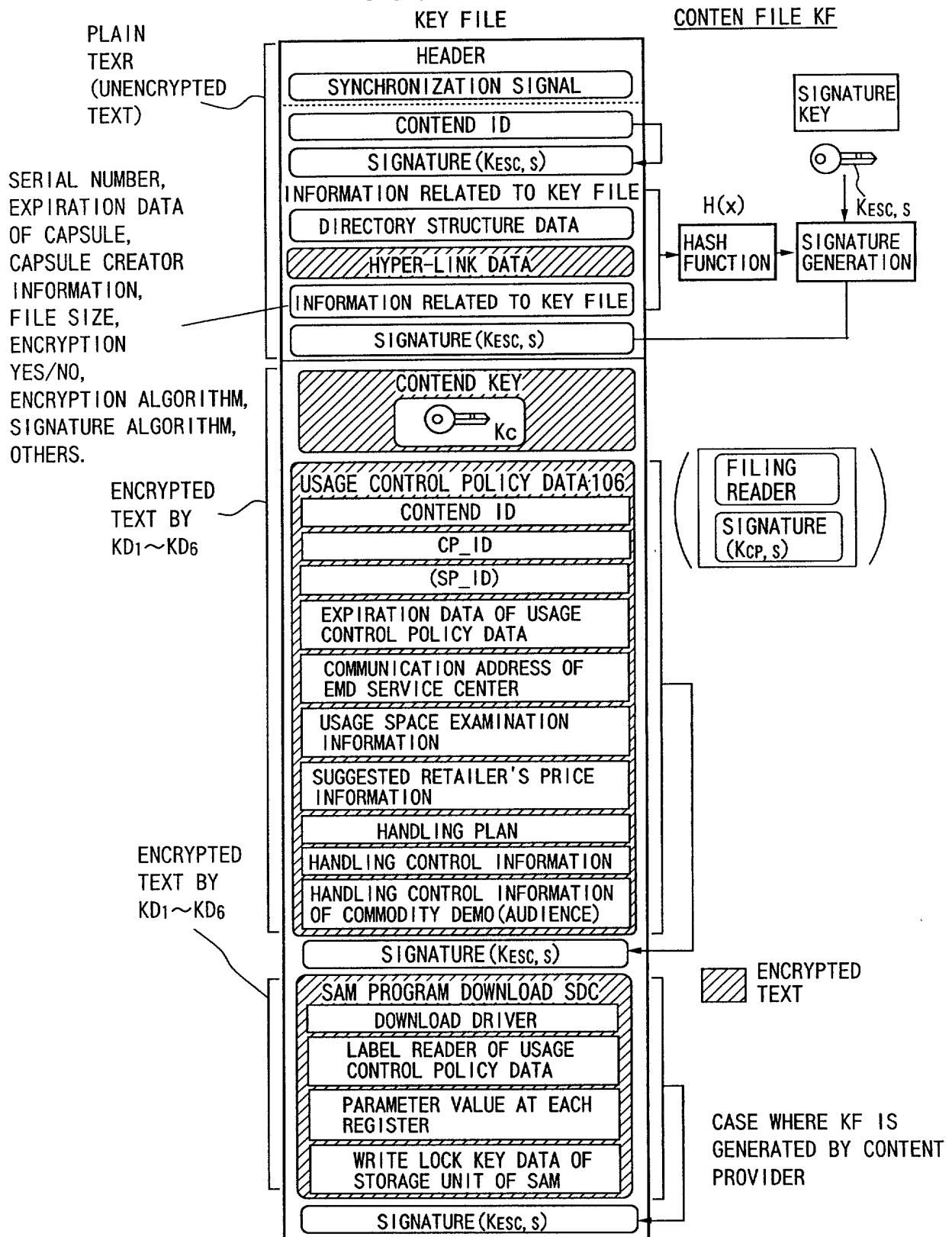
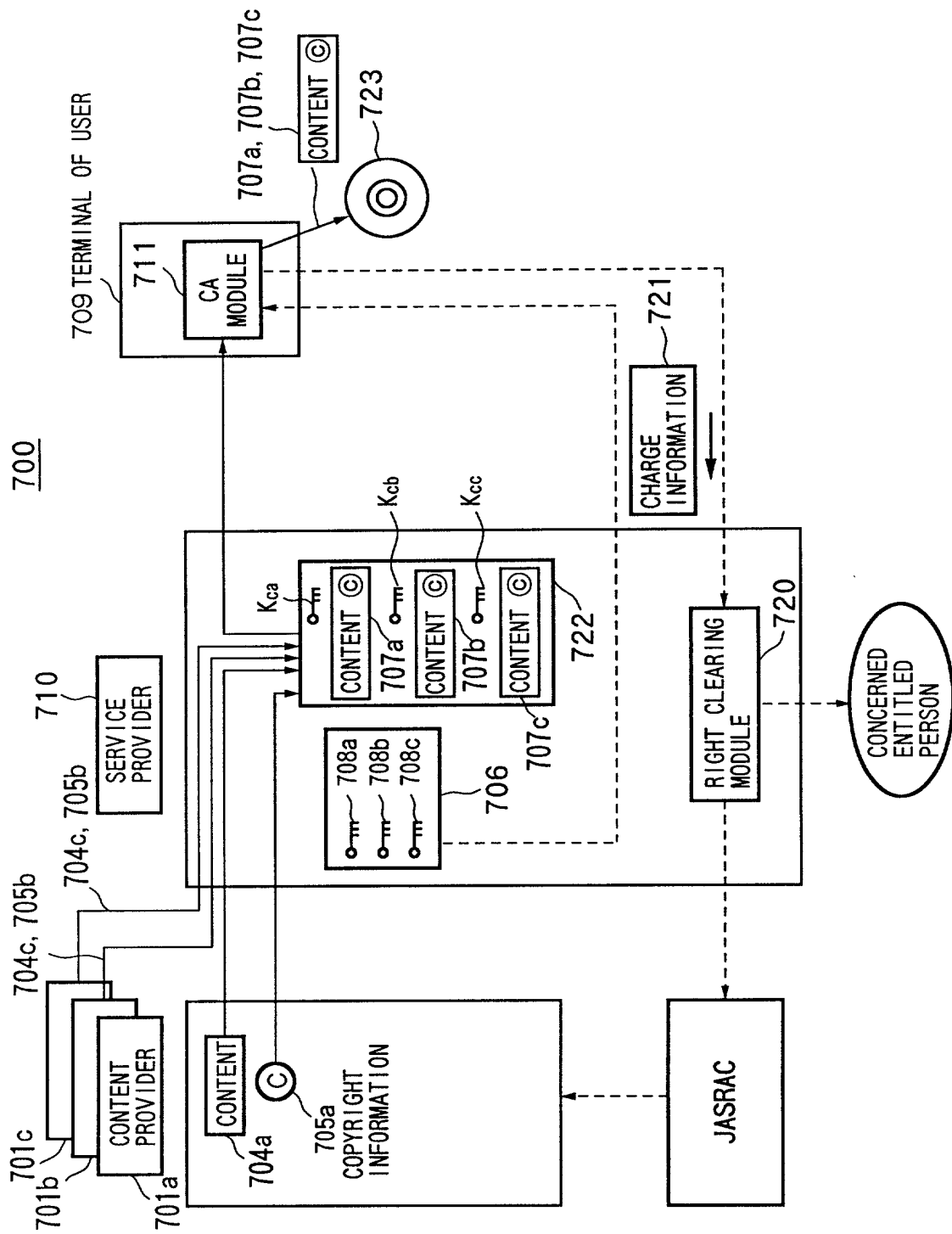


FIG. 145

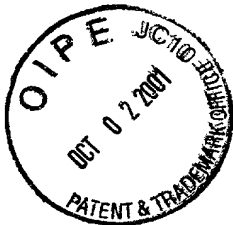


## LIST OF REFERENCE NUMERALS

90... payment gateway  
91... settlement manager  
92... route certificate authority  
100, 300... EMD system  
101, 301... content provider  
102, 302... EMD service center  
103, 303... user home network  
104, 304... secure container  
105<sub>1</sub> to 105<sub>4</sub>, 305<sub>1</sub> to 305<sub>4</sub>... SAM  
106... usage control policy data  
107, 307... settlement report data  
108, 308... usage log data  
160<sub>1</sub>... network apparatus  
160<sub>2</sub> to 160<sub>4</sub>... AV apparatuses  
152, 152c, 152s... settlement claim data  
191... bus  
310... service provider  
311... CA module  
312... price tag data  
CF... content file  
KF... key file  
Kc... content key data

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

特許出願宣言書及び委任状



Japanese Language Declaration

日本語宣言書

Attorney Docket No. 9798423-0006

下記の氏名の発明者として、私は以下の通り宣言します。

私の住所、私書箱、国籍は下記の私の氏名の後に記載された通りです。

下記の名称の発明に関して請求範囲に記載され、特許出願している発明内容について、私が最初かつ唯一の発明者（下記の氏名が一つの場合）もしくは最初かつ共同発明者であると（下記の名称が複数の場合）信じています。

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

"Data Providing System and Method  
~~Therefor~~ of Same"

上記発明の明細書（下記の欄でx印がついていない場合は、本書に添付）は、

the specification of which is attached hereto unless the following box is checked:

☐ \_\_月\_\_日に提出され、米国出願番号または特許協定条約国際出願番号を\_\_\_\_とし、  
（該当する場合）\_\_\_\_に訂正されました。

☐ was filed on \_\_\_\_\_ as United States Application Number or PCT International Application Number and was amended on \_\_\_\_\_ (if applicable)

私は、特許請求範囲を含む上記訂正後の明細書を検討し、内容を理解していることをここに表明します。

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

私は、連邦規則法典第37編第1条56項に定義されたとおり、特許資格の有無について重要な情報を開示する義務があることを認めます。

I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56.

私は、米国法典第35編119条(a)-(d)項又は365条(b)項に基づき下記の、米国以外の国の少なくとも一カ国を指定している特許協力条約365(a)項に基づき国際出願、又は外国での特許出願もしくは発明者証の出願についての外国優先権をここに主張するとともに、優先権を主張している、本出願の前に出願された特許または発明者証の外国出願を以下に、枠内をマークすることで、示しています。

Prior Foreign Application(s)

外国での先行出願

11-309722 Japan 17 09 1999

(Number) (番号)	(Country) (国名)	(Day Month Year Filed) (出願年月日)
11-309721	Japan	17 09 1999

(Number) (番号)	(Country) (国名)	(Day Month Year Filed) (出願年月日)
PCT/JP00/06308	WO	14 09 2000

私は、第35編米国法典119条(e)項に基づいて下記の米国特許出願規定に記載された権利をここに主張いたします。

(Application No.) (出願番号)	(Filing Date) (出願日)
-----------------------------	------------------------

私は、下記の米国法典第35編120条に基づいて下記の米国特許出願に記載された権利、又は米国を指定している特許協力条約365条(c)に基づき権利をここに主張します。また、本出願の各請求範囲の内容が米国法典第35編112条第1項又は特許協力条約で規定された方法で先行する米国特許出願に開示されていない限り、その先行米国出願書提出日以降で本出願書の日本国内または特許協力条約国際提出日までの期間中に入手された、連邦規則法典第37編1条56項で定義された特許資格の有無に関する重要な情報について開示義務があることを認識しています。

I hereby claim foreign priority under Title 35, United States Code, Section 119(a)-(d) or 365(b) of any foreign application(s) for patent or Inventor's certificate or 365(a) of any PCT International application which designated at least one country other than the United States, listed below and have also identified below, by checking the box, any foreign application for patent or Inventor's certificate or PCT International application having a filing date before that of the application on which priority is claimed:

Priority Claimed

優先権主張なし

(Number)	(Country)	(Day Month Year Filed)
----------	-----------	------------------------

(Number)	(Country)	(Day Month Year Filed)
----------	-----------	------------------------

I hereby claim the benefit under Title 35, United States Code, Section 119(e) of any United States provisional application(s) listed below.

(Application No.) (出願番号)	(Filing Date) (出願日)
-----------------------------	------------------------

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States application(s) or 365(c) of an PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of Title 35, United States Code, Section 112, I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56 which became available between the filing date of the prior application and the national or PCT International filing date of this application.

Page 6

Page 6

Japanese Language Declaration

(日本語宣言書)



(Application No.)  
[出願番号]

(Filing Date)  
[出願日]

(Status: patented, pending, abandoned)  
{現況: 特許許可済, 係属中, 放棄済}

Application No.)  
[出願番号]

(Filing Date)  
[出願日]

(Status: patented, pending, abandoned)  
{現況: 特許許可済, 係属中, 放棄済}

私は、私自身の知識に基づいて本宣言書中で私が行なう表明が真実であり、かつ私の入手した情報と私の信じることに基づく表明が全て真実であると信じていること、さらに故意になされた虚偽の表明及びそれと同等の行為は米国法典第18編第1001条に基づき、罰金または拘禁、もしくはその両方により処罰されること、そしてそのような故意による虚偽の声明を行なえば、出願した、又は既に許可された特許の有効性が失われることを認識し、よってここに上記のごとく宣誓を致します。

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

委任状: 私は下記の発明者として、本出願に関する一切の手続きを米特許商標局に対して遂行する弁理士または代理人として、下記の者を指名いたします。(弁理士、または代理人の氏名及び登録番号を明記のこと)

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. (list name and registration number)

David R. Metzger (Reg. No. 32,919), Jordan A. Sigale, (Reg. No. 39,028), Michael A. Molano (Reg. No. 39,777), Michael L. Kiklis (Reg. No. 38,939), Janelle D. Strode (Reg. No. 34,738), Kevin W. Guynn (Reg. No. 29,972), Jennifer Hammond (Reg. No. 41,814), Lana Knedlik (Reg. No. 42,748), John F. Griffith (Reg. No. 44,137), Marina Saito (Reg. No. 42,121), Alison P. Schwartz (Reg. No. 43,863), Christopher P. Rauch (Reg. No. 45,034), Francisco Rubio-Campos (Reg. No. 45,358), Brian J. Gill (Reg. No. 46,727), Gregory B. Gulliver, Reg. No. 44,138 and Shashank S. Upadhye, all members of the firm of Sonnenschein, Nath & Rosenthal

Send Correspondence to:

書類送付先

David R. Metzger  
Sonnenschein Nath & Rosenthal  
P.O. Box #061080  
Wacker Drive Station  
Chicago, Illinois 60606-1080

直接電話連絡先: (名前及び電話番号)

Direct Telephone Calls to: (name and telephone number)

312/876-2578

Page 7  
Page 7

Japanese Language Declaration

(日本語宣言書)

唯一または第一発明者名	Full name of sole or first inventor: Akira Nonaka	
発明者の署名	Inventor's signature <i>Akira Nonaka</i>	Date June, 11, 2001
住所	Residence Kanagawa, Japan	
国籍	Citizenship Japan	
私書箱	Post Office Address c/o Sony Corporation 7-35, Kitashinagawa 6-chome Shinagawa-ku, Tokyo 141, Japan	

(第三以降の共同発明者についても同様に記載し、署名をすること)

第二共同発明者	Full name of second joint inventor, if any Tadashi Ezaki	
発明者の署名	Inventor's signature	Date
住所	Residence	
国籍	Citizenship Japan	
私書箱	Post Office Address c/o Sony Corporation 7-35, Kitashinagawa 6-chome Shinagawa-ku, Tokyo 141, Japan	
第二共同発明者	Full name of third joint inventor, if any:	
発明者の署名	Inventor's signature	Date
住所	Residence	
国籍	Citizenship	
私書箱	Post Office Address	

## Japanese Language Declaration

(日本語宣言書)

唯一または第一発明者名	Full name of sole or first inventor: Akira Nonaka
発明者の署名 日付	Inventor's signature Date
住所	Residence
国籍	Citizenship Japan
私書箱	Post Office Address c/o Sony Corporation 7-35, Kitashinagawa 6-chome
	Shinagawa-ku, Tokyo 141, Japan

(第三以降の共同発明者についても同様に記載し、署名をすること)

第二共同発明者	Full name of second joint inventor, if any Tadashi Ezaki
発明者の署名 日付	Inventor's signature Date Tadashi Ezaki June 4, 2001
住所	Residence Tokyo, Japan
国籍	Citizenship Japan
私書箱	Post Office Address c/o Sony Corporation 7-35, Kitashinagawa 6-chome
	Shinagawa-ku, Tokyo 141, Japan
第二共同発明者	Full name of third joint inventor, if any:
発明者の署名 日付	Inventor's signature Date
住所	Residence
国籍	Citizenship
私書箱	Post Office Address